

Natalie Lyons, No. 293026
 Vess A. Miller, No. 278020
 COHENMALAD, LLP
 One Indiana Square, Suite 1400
 Indianapolis, Indiana 46204
 Tel: (317) 636-6481
 nlyons@cohenmalad.com
 vmiller@cohenmalad.com

*To move for *pro hac vice* admission
 [additional counsel listed on signature pages]

Counsel for Plaintiff and the Proposed Class

**UNITED STATES DISTRICT COURT
 NORTHERN DISTRICT OF CALIFORNIA
 OAKLAND DIVISION**

**MARTIN BELTRAN, individually and on
 behalf of all others similarly situated,**

Plaintiff

v.

**NATIONSTAR MORTGAGE LLC d/b/a
 MR. COOPER,**

Defendant.

Civil Action No. 3:25-cv-04412-JSC

AMENDED CLASS ACTION

COMPLAINT FOR:

- 1. Negligence**
- 2. Violation of Comprehensive Computer Data Access and Fraud Act, Cal. Pen. Code § 502**
- 3. Violation of Consumer Protection Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.***
- 4. Violation of Consumer Privacy Act, Cal. Civ. Code, §§ 1798.100, *et seq.***
- 5. Breach of Express and Implied Contract**
- 6. Unjust Enrichment**
- 7. Breach of Confidence**
- 8. Violation of Invasion of Privacy Act, Cal. Pen. Code §§ 631, *et seq.***
- 9. Violation of Invasion of Privacy Act, Cal. Pen. Code §§ 632, *et seq.***
- 10. Violation of Invasion of Privacy Act, Cal. Pen. Code §§ 638.51, *et seq.***
- 11. Violations of the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. §§ 2511(1), *et seq.***

DEMAND FOR JURY TRIAL

AMENDED CLASS ACTION COMPLAINT

Plaintiff Martin Beltran, individually and on behalf of all others similarly situated (hereinafter “Plaintiff”) brings this Amended Class Action Complaint against Defendant, Nationstar Mortgage LLC d/b/a Mr. Cooper (“Mr. Cooper” or “Defendant”), and alleges, upon personal knowledge as to his own actions, and upon information and belief as to all other matters, as follows.

INTRODUCTION

1. Plaintiff brings this class action to address Defendant’s outrageous, illegal, and widespread practice of disclosing—without consent—the Nonpublic Personal Information¹ and Personally Identifiable Financial Information² (together, “Personal and Financial Information”) of Plaintiff and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta (“Facebook” or “Meta”), Google, LLC (“Google”), Microsoft Corp. (“Microsoft”), DoubleClick, NewRelic, Optimizely, HotJar, and possibly others (collectively the “Third Parties”) (in short, “the Disclosure”).

2. Mr. Cooper is a massive mortgage lender and servicer that provides services to customers across the globe and the United States, including in California. To provide these services, Mr. Cooper operates and encourages its customers to use its website,

¹ The United States Congress defines “nonpublic personal information” as “personally identifiable financial information-- (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.” The Gramm-Leach-Bliley Act, 15 U.S.C.A. § 6809(4)(A) (“GLBA”).

² “Personally identifiable financial information means any information: (i) A consumer provides to [a financial institution] to obtain a financial product or service from [the financial institution]; (ii) About a consumer resulting from any transaction involving a financial product or service between [a financial institution] and a consumer; or (iii) [a financial institution] otherwise obtain[s] about a consumer in connection with providing a financial product or service to that consumer.” 16 C.F.R. § 313.3(o)(1).

1 <https://www.mrcooper.com/> (the “Website”), on which customers can, among other things, access
 2 their account information, manage their mortgage, obtain information about Mr. Cooper’s services,
 3 calculate and obtain quotes for mortgage payments and refinancing options, and apply mortgages
 4 or refinancing.
 5

6 3. Despite its unique position as a massive and trusted mortgage lender and servicer,
 7 Mr. Cooper used its Website to blatantly collect and disclose Consumers’³ and Customers’⁴
 8 (collectively, “Customers”) Personal and Financial Information to Third Parties uninvolved in the
 9 provision of mortgage services—entirely without their knowledge or authorization. Mr. Cooper
 10 did so by knowingly and secretly configuring and implementing code-based tracking devices
 11 (“trackers” or “tracking technologies”) into its Website.
 12

13 4. Through these trackers, Mr. Cooper disclosed and continues to disclose Personal
 14 and Financial Information that Customers input into and accessed on Mr. Cooper’s Website. This
 15 information includes without limitation, the user’s status as a customer; whether the customer is
 16 logged in to Mr. Cooper’s website; the user’s browsing activities, including that the user clicked
 17 certain buttons and what URLs or webpages they led to; the user’s refinancing options and
 18 customer selection; the reason the customer is seeking to refinance; that the user submitted a
 19 mortgage and/or refinancing application; the user’s request for a quote and a summary of the user’s
 20 selections; the type of property at issue; the state where the user’s property is located; and the
 21
 22
 23

24 ³ The term “consumer” means “an individual who obtains or has obtained a financial
 25 product or service . . . that is to be used primarily for personal, family, or household purposes, or
 26 that individual’s legal representative.” 16 C.F.R. § 313.3; 15 U.S.C.A. § 6809(9).

27 ⁴ “Customer means a consumer who has a customer relationship with [a financial
 28 institution].” 16 C.F.R. § 313.3. “The term ‘time of establishing a customer relationship’ shall . . .
 in the case of a financial institution engaged in extending credit directly to consumers to finance
 purchases of goods or services, mean the time of establishing the credit relationship with the
 consumer.” 15 U.S.C.A. § 6809.

1 user's current stage of the homebuying process.

2 5. Upon information and belief, Mr. Cooper utilized data from trackers to improve
3 and to save costs on its marketing campaigns, improve its data analytics, attract new customers,
4 and generate sales. Mr. Cooper benefited from use of Customers' Personal and Financial
5 Information. Mr. Cooper further allowed the Third Parties, who are uninvolved in Mr. Cooper's
6 provision of mortgage services, to profit from its Disclosure of Customers' Private and Financial
7 information. And the Third Parties used Customers' Personal and Financial Information for
8 themselves and disclosed to fourth parties who also profited off of it. Facebook, for example, will
9 use the data collected from Customers of Mr. Cooper to sell ads to fourth parties who will further
10 profit off the use of that information

11 6. Customers like Plaintiff and Class Members simply do not anticipate that a trusted
12 mortgage lender and servicer will send their Personal and Financial Information to hidden Third
13 Parties (who in turn share with fourth parties), all of whom profit off of it. Likewise, when Plaintiff
14 and Class Members used Defendant's Website, they thought they were communicating exclusively
15 with a trusted mortgage lender and servicer for the sole purpose of obtaining mortgage information
16 and/or services.

17 7. At no time did Mr. Cooper disclose to Plaintiff or Class Members that it was sharing
18 their Personal and Financial Information with the Third Parties for third- and fourth-party use.
19 Plaintiff and Class Members never signed a written authorization permitting Defendant to send
20 their Personal and Financial Information to the Third Parties who were uninvolved in the provision
21 of financial services.

22 8. Defendant owed a variety of duties, including common law, statutory, contractual,
23 and regulatory duties, to keep Plaintiff's and Class Members' Personal and Financial Information
24
25
26
27
28

1 safe, secure, and confidential.

2 9. Furthermore, by obtaining, collecting, using, and deriving a benefit from
3 Plaintiff's and Class Members' Personal and Financial Information, Defendant assumed legal and
4 equitable duties to those individuals to protect and safeguard their information from unauthorized
5 disclosure.
6

7 10. The statutory and regulatory duties Mr. Cooper owed Customers include its
8 obligations under federal law. For example, the GLBA requires that "each financial institution has
9 an affirmative and continuing obligation to respect the privacy of its customers and to protect the
10 security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. §
11 6801. Under this federal law, financial institutions like Mr. Cooper are explicitly prohibited from
12 disclosing a Customer's Personal and Financial Information without sufficient advance
13 notification and opt-out opportunity. 15 U.S.C. § 6801, *et seq.*
14

15 11. Mr. Cooper ignored all its duties and obligations, including the GLBA's
16 requirements, by disclosing Customers' Personal and Financial Information without proper
17 advance notification and opt-out rights as required under the GLBA.
18

19 12. Examples of "Personal and Financial Information" included in the GLBA are
20 indistinguishable from the types of information Mr. Cooper disclosed to Facebook, Google, and
21 Microsoft, including, among other things: (a) "[i]nformation a consumer provides to [Mr. Cooper]
22 on an application to obtain a loan, credit card, or other financial product or service"; (b) "[t]he fact
23 that an individual is or has been one of [Mr. Cooper's] customers or has obtained a financial
24 product or service from [Mr. Cooper]"; (c) "information about [Mr. Cooper] consumer . . .
25 disclosed in a manner that indicates that the individual is or has been [Mr. Cooper] consumer"; and
26 (d) "any information [Mr. Cooper] collect[s] through an Internet 'cookie' (an information
27
28

collecting device from a web server).” 16 C.F.R. 313.3(o)(2)(i).

13. Mr. Cooper breached its duties under California state law, including, for example, the California Consumer Privacy Act. That statute provides California consumers with rights to control their personal information including the right to know what personal information is being collected about them and whether that information is sold or disclosed and to whom, the right to prohibit the sale of their personal information, and the right to request deletion of their personal information. Cal. Civ. Code § 1798.100, *et seq.* Mr. Cooper breached its obligations under this statute by, for example, failing to provide Customers with appropriate notice that their information was being disclosed to Third Parties for third- and fourth- party use. The notice and consent Mr. Cooper purports to provide and obtain, through the policies it provides on its website, is not appropriate or sufficient, as a reasonable Consumer would not have understood those policies as notifying them of Mr. Cooper’s disclosure of their Personal and Financial Information to Third Parties for third- and fourth- party use.

14. Mr. Cooper breached its common law, statutory, and contractual obligations to Plaintiff and Class Members by, *inter alia*, (i) failing to adequately review its marketing programs and web based technology to ensure its Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to collect and share Personal and Financial Information; (iii) aiding, agreeing, and conspiring with the Third Parties to intercept communications sent and received by Plaintiff and Class Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to disclose their Personal and Financial Information to Third Parties for Third Party and fourth party use; (v) failing to protect Personal and Financial Information and take steps to block the transmission of Plaintiff’s and Class Members’ Personal and Financial Information through the use of tracking technology; (vi) failing to warn Plaintiff and

1 Class Members; and (vii) otherwise failing to design and monitor its Website to maintain the
2 confidentiality and integrity of its customers' Personal and Financial Information.

3
4 15. Plaintiff seeks to remedy these harms and brings causes of action of Negligence;
5 Violation of the Comprehensive Computer Data Access And Fraud Act ("CDAFA"), Cal. Penal
6 Code § 502; Violation Of California's Consumer Protection Law ("UCL"), Cal. Bus. & Prof. Code
7 §§ 17200, *et seq.*; Violation of California Consumer Privacy Act ("CCPA"), 1798.100, *et seq.*;
8 Breach of Express and Implied Contract; Unjust Enrichment; Breach Of Confidence; Violation of
9 The California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 631, *et seq.*; Violation of
10 Invasion of Privacy Act, Cal. Pen. Code §§ 632, *et seq.*; Violation of Invasion of Privacy Act, Cal.
11 Pen. Code §§ 638.51, *et seq.*; and Violation of The Electronic Communications Privacy Act
12 ("ECPA"), 18 U.S.C. §§ 2511(1), *et seq.*
13

14 16. Plaintiff brings this action, individually and on behalf of all others similarly
15 situated, for damages and equitable relief.
16

17 PARTIES

18 17. Plaintiff Martin Beltran is a natural person and citizen of California, where he
19 intends to remain. Plaintiff Beltran resides in Vallejo, Solano County, California. Plaintiff Beltran
20 has a mortgage with Mr. Cooper and is a victim of Defendant's unauthorized Disclosure of
21 Personal and Financial Information.
22

23 18. Defendant Nationstar Mortgage LLC d/b/a Mr. Cooper is a Delaware corporation
24 that services mortgage loans. Defendant has its principal place of business in Coppel, Texas.
25 Defendant transacts or has transacted business in this District and throughout the United States,
26 including through its office in Lake Forest, California.
27

28 19. Mr. Cooper is a financial institution, as that term is defined by Section 509(3)(A)

of the GLBA, 15 U.S.C. § 6809(3)(A).

JURISDICTION AND VENUE

20. This Court has personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business in this State, maintains corporate offices in California, and committed tortious acts in this State.

21. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds \$5,000,000, exclusive of interest and costs. Complete diversity exists between Defendant and at least one member of the proposed Classes, and there are more than one hundred (100) members in the proposed Classes.

22. This Court also has subject matter jurisdiction under 28 U.S.C. § 1331 because it arises under the laws of the United States. The Court has supplemental jurisdiction over Plaintiff's claims arising under state law pursuant to 28 U.S.C. § 1367.

23. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this district and continue to occur in this district.

COMMON FACTUAL ALLEGATIONS

A. Mr. Cooper: A Dominant Mortgage Lender and Servicer that Collects Personal and Financial Information Under the Guise of Protecting it

24. Nationstar Mortgages, LLC, is the consumer-facing mortgage lender and servicer that operates under the service mark "Mr. Cooper."

25. Mr. Cooper provides "servicing, origination, and transaction-based services related principally to single-family residents throughout the United States."⁵ "Serving 6.5 million

⁵ *About our Leaders*, MR. COOPER, <https://www.mrcooper.com/about-us/leadership> (last accessed May 12, 2025).

1 homeowners, Mr. Cooper is one of the largest home loan servicers in the country.”⁶

2 26. Frequently, home buyers and homeowners are introduced to Mr. Cooper after their
3 mortgage is sold or assigned to the company for servicing.
4

5 27. On information and belief, Mr. Cooper provides mortgage services to Customers in
6 every state in America.

7 28. Mr. Cooper represents to its customers that it “take[s] your privacy seriously.”⁷

8 29. Through its Website, Mr. Cooper allows users to explore various services relating
9 to their mortgages and home loans such as home equity loans, cash-out refinancing, refinancing to
10 lower monthly payments, applying for pre-approval and verified approval, loan applications and
11 loan approval, and selling homes.⁸
12

13 30. Mr. Cooper’s Website also encourages to use various mortgage calculators through
14 which they can enter their personal and financial information to calculate their estimated payments,
15 payoff amounts, qualifying loan amounts, refinancing options, homebuying budget, and options
16 for renting versus buying a home.⁹ In short, Defendant encourages customers to use its Website
17 to apply for, manage, and access their mortgages and accounts.
18

19 31. Defendant encourages the use of its Website in service of its own goal of increasing
20 profitability. In furtherance of that goal, Defendant purposely and secretly installed the Third
21 Parties’ online tracking technology onto its Website to gather and share information about
22

23
24 ⁶ *About Us: Purpose & Value*, MR. COOPER, <https://www.mrcooper.com/about-us/purpose> (last accessed May 12, 2025).

25 ⁷ *Terms and Conditions*, MR. COOPER, https://www.mrcooper.com/terms_of_use (last
26 accessed May 12, 2025).

27 ⁸ See *Home Loan Types*, MR. COOPER, https://www.mrcooper.com/loans/types?internal_ref=loan_types_leftnav (last accessed May 12,
28 2025).

⁹ See *Mortgage Calculators*, MR. COOPER, <https://www.mrcooper.com/calculators> (last
accessed May 12, 2025).

1 Customers.

2 32. Mr. Cooper utilized the information it collected to market its services and bolster
3 its profits by surreptitiously diverting the information to Third Parties like Google and Facebook.
4

5 33. But Defendant did not only collect information for its own use; Defendant also
6 shared—and continues to share—Customers' information, including Personal and Financial
7 Information, with the unauthorized Third Parties who then use it for their own benefit and to
8 benefit fourth parties who are even further removed from the Customers.
9

10 **B. Third Parties and Trackers: Collectors and Profiteers of Personal and Financial
11 Information**

12 34. The invisible Third Party online tracking technologies installed by Mr. Cooper on
13 its Website gathers a vast assortment of Customer data. The installation of these trackers—and
14 thus their transmission of data—is in Mr. Cooper's exclusive control.

15 35. When an individual accesses a webpage containing online tracking technology
16 from a Third Party, the trackers instantaneously and surreptitiously duplicate communications with
17 that webpage and send them to the Third Party. The information travels directly from both the
18 user's browser and the webpage owner's server and then on to the Third Party's server, based off
19 instructions from the Third Party's tracker. The communications and information transmitted via
20 these trackers are entirely in Defendant's control. Customers trust Mr. Cooper with the information
21 they input on Mr. Cooper's Website, and Mr. Cooper is in complete and exclusive control of its
22 Website and the data input therein.
23

24 36. Online tracking technologies may not be deleted from an individual's device; they
25 are built into a webpage, and a Customer has no control or warning over their presence on the
26 webpage or that they collect certain data. Third party trackers cause information to flow directly
27 from the website Customer's browser and the website owner's server to the Third Party itself. A
28

1 webpage Customer cannot prevent or even detect this transmission of data.

2 37. Accordingly, without any knowledge, authorization, or action by a user, a website
3 owner who has installed Third Party trackers is utilizing website source code to commandeer its
4 users' computing devices and web browsers, causing them to invisibly re-direct the users'
5 communications to Third Parties.
6

7 38. In this case, Defendant employed the Third Party trackers to intercept, duplicate,
8 and re-direct Plaintiff's and Class Members' Personal and Financial Information to the Third
9 Parties contemporaneously, invisibly, and without the customer's knowledge.
10

11 39. Consequently, when Plaintiff and Class Members visited Defendant's Websites and
12 communicated their Personal and Financial Information, that information was simultaneously
13 intercepted and transmitted to the Third Parties.
14

15 40. The Third Party trackers do not provide any substantive content on Mr. Cooper's
16 Website. Their only purpose is to collect and share information to be used for the Third Party and
17 fourth parties' marketing and sales purposes.

18 41. The Facebook or Meta Pixel, for example, "tracks the people and type of actions
19 they take" on a website.¹⁰ It can be used to gather customer data, identify customers and potential
20 customers, target advertisements to those individuals, and market products and services. This
21 includes when a user visits a particular webpage, clicks a button, fills out a form (including the
22 information from the form like the state in which the property is located, the reason the customer
23 is seeking to refinance, etcetera), IP addresses, web browser information, page location, any
24
25
26
27

28 ¹⁰ *Retargeting*, Meta, <https://www.facebook.com/business/goals/retargeting> (last visited Aug. 11, 2024).

1 custom events set by the website owner, the tracker ID, and more.¹¹ Facebook does all of this by
2 using the Meta Pixel to send “events” to its server.

3
4 42. Once the data is collected via the Meta Pixel, Facebook aggregates it to build its
5 own massive, proprietary dataset, which Facebook then uses to find new customers, drive sales,
6 and understand ad impact. This is all to the benefit of the website owner, like Mr. Cooper, Facebook
7 as the third party, and other fourth parties, all of whom use the information for targeted marketing
8 campaigns. Targeting works by allowing fourth parties to direct their ads at particular “Audiences,”
9 subsets of individuals who, according to Facebook, are the “people most likely to respond to your
10 ad.”¹²

11
12 43. Upon information and belief, the Meta Pixel installed on Mr. Cooper’s website
13 collects data including the “c_user cookie,” which enables Facebook to link the user to their logged
14 in Facebook account and thereby identify the user. The Meta Pixel has also reported information
15 such as when the user visited the page for “loantype=get-cash,” when the user submits an online
16 application or completes a registration, and has historically reported to Facebook that the user was
17 on a page for “simple-cash-options” when the user loads the page for “Getting Cash from Equity.”

18
19 44. Data harvesting is big business for Facebook; it drives Facebook’s advertising sales,
20 which are its profit center. In 2023, Facebook generated nearly \$135 billion in revenue, roughly
21

22
23
24
25 ¹¹ See, e.g., *Meta Pixel*, Meta for Developers, [https://developers.facebook.com/docs/meta-](https://developers.facebook.com/docs/meta-pixel/)
26 [pixel/](https://developers.facebook.com/docs/meta-pixel/) (last visited Aug. 11, 2024); *Specifications for Facebook Pixel Standard Events*, Meta,
27 <https://www.facebook.com/business/help/402791146561655> (last visited Aug. 11, 2024); see also
28 *Facebook Pixel, Accurate Event Tracking, Advanced*, Meta for Developers
<https://developers.facebook.com/docs/facebook-pixel/advanced/> (last visited Aug. 11, 2024).

¹² *Audience Ad Targeting*, Meta, <https://www.facebook.com/business/ads/ad-targeting>
(last visited Aug. 14, 2023).

98% of which was derived in advertising revenue alone space.¹³ This business model is not limited to Facebook. Data harvesting one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the “new oil.”¹⁴ Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 were as high as \$434 per user, for a total of more than \$200 billion industry wide. The updated 2025 numbers show “the annual value of your data if you live in the US is at least \$700” per user.¹⁵

45. On information and belief, the trackers Defendant installed from other Third Parties, including Google, Microsoft, DoubleClick, New Relic, Optimizely, and HotJar, work similarly to the Meta Pixel and likewise transmitted Plaintiff’s and the Class Members’ Personal and Financial Information without Plaintiff’s and Class Members’ knowledge or authorization.

46. The Google trackers allow Defendant to track and share with Google (1) who uses Mr. Cooper’s Website; (2) whether the user is a customer of Mr. Cooper; (3) what actions the user performs on the Website such as what types of products the customer is viewing as well as the customer’s selections on those pages, including the reason for the user’s request; (4) when users visit the Website; (5) where on the website users perform these actions; and (6) how users navigate through the website to perform these actions. Google gathers this information using trackers embedded on Mr. Cooper’s Website and generates corresponding reports.¹⁶ DoubleClick is part of

¹³ *Meta Reports Fourth Quarter and Full Year 2023 Results*, Facebook <https://investor.fb.com/investor-news/press-release-details/2024/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend/default.aspx> (last visited Aug. 8, 2024).

¹⁴ What’s your data really worth? (2025 update) | Proton, <https://proton.me/blog/what-is-your-data-worth> (last visited Sept. 8, 2025).

¹⁵ *Id.*

¹⁶ *See generally, A big list of what Google Analytics can & cannot do*, MarketLyrics, <https://marketlyrics.com/blog/list-of-things-google-analytics-can-and-cannot-do/> (last accessed May 12, 2025).

the suite Google uses to collect all of this.¹⁷ Google’s collection of this data “enables advertisers to more effectively create, manage and grow high-impact digital marketing campaigns.”¹⁸

47. The Microsoft tracker allows Defendant to “[t]rack what your customers are doing after they click on your ad.”¹⁹ According to Microsoft, the tracker “records what customers do on your website . . . [and] will collect data that allows you to track conversion goals and target audiences with remarketing lists.”²⁰

48. The New Relic tracker is an application performance management tool, used for application monitoring, which can track every action a user performs on the website.²¹

49. The Optimizely tracker is a ‘post-click tracking’ file that is automatically “loaded from a server when a customer clicks on a link” and “will not be noticed” by users.²² “One [Optimizely] tracking pixel can transmit up to 19 values.”²³

50. Similarly, “[t]he Hotjar Tracking Code is used to trigger data collection when installed” and “is responsible for collecting and sending the data to” whichever Third Party installed the code.²⁴

¹⁷ See the *DoubleClick Digital Marketing Suite*, Google Developers, <https://developers.google.com/app-conversion-tracking/third-party-trackers/doubleclick> (last accessed May 12, 2025).

¹⁸ See *DoubleClick Digital Marketing*, Google Help, <https://support.google.com/faqs/answer/2727482?hl=en> (last accessed May 12, 2025).

¹⁹ *Microsoft Advertising*, Microsoft.com, [https://about.ads.microsoft.com/en/tools/performance/conversion-tracking#:~:text=Universal%20Event%20Tracking%20\(UET\)%20is,target%20audiences%20with%20remarketing%20lists](https://about.ads.microsoft.com/en/tools/performance/conversion-tracking#:~:text=Universal%20Event%20Tracking%20(UET)%20is,target%20audiences%20with%20remarketing%20lists) (last visited June 26, 2024).

²⁰ *Id.*

²¹ *Monitor, Debug and Improve Your Entire Stack*, New Relic, <https://newrelic.com/> (last visited Aug. 8, 2024).

²² *Post-Click Tracking*, OPTIMIZELY, <https://support.optimizely.com/hc/en-us/articles/4413205550733-Post-click-tracking> (last visited May 13, 2025).

²³ *Id.*

²⁴ *What is the Hotjar Tracking Code?*, HOTJAR, <https://help.hotjar.com/hc/en-us/articles/115011639927-What-is-the-Hotjar-Tracking-Code> (last accessed May 11, 2025).

51. Hotjar code, like the other trackers discussed herein, requires “administrative access to the web hosting of [the] site [the Third Party] want[s] to track” as well as “the ability to insert the Hotjar tracking code into the HTML of [the] pay [the Third Party] want[s] to track. This requires that [the Third Party] either own[s] the site or ha[s] explicit permission from the site owner to edit it.”²⁵

52. The collection and disclosure of users’ data via these trackers occurs automatically.

C. Mr. Cooper Used Trackers to Disclose Personal and Financial Information Without Users’ Authorization.

53. On information and belief, Mr. Cooper installed each of these trackers, through which Mr. Cooper transmitted Customers’ communications with Mr. Cooper’s website and thus their Personal and Financial Information to the Third Parties without Customers’ knowledge or authorization. This information included their browsing activities including the pages they viewed and the buttons they clicked; information revealed in the application process regarding (i) the products in which Customers were interested, (ii) the reason they were seeking the product, (iii) the user’s status as a Mr. Cooper customer, and (iv) information about the Customer’s property and application, including, without limitation, the Customer’s stage in the home buying and/or selling process, the type of property at issue, and the state in which the property is located.

54. On information and belief, since at least May 25, 2019, and at least as recently as May 5, 2025, Mr. Cooper has had tracking technologies installed on its Website.

55. Accordingly, Mr. Cooper disclosed its Customers’ data and Personal and Financial Information to the Third Parties, like Facebook, beginning some time prior to May 2019 and

²⁵ *Platforms and Frameworks Not Compatible with Hotjar*, HOTJAR, <https://help.hotjar.com/hc/en-us/articles/115012499507-Platforms-and-Frameworks-Not-Compatible-with-Hotjar> (last accessed May 11, 2025).

1 continuing up until at least May 2025.

2 56. The information and data collected by these trackers allowed Third Parties like
3 Meta, Google, and Microsoft to identify individual users and link those Customers to other online
4 accounts, such as the Customer's Facebook account.
5

6 *i. Mr. Cooper Installed Meta Pixels to Track Customers' Browsing Activities Across its*
7 *Website.*

8 57. Mr. Cooper discloses Customers' information to Meta via a Meta Pixel with ID
9 1498188900425660:
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

The screenshot displays the Mr. Cooper website interface and its network traffic. The website has a green header with the 'mrcooper.com' logo and a 'Sign In' button. The main content area features a 'Get More from Your Mortgage' section with a 'Call Us' button and a 'See The Benefits' button. Below this is a 'Home Shopping Should Be Exciting' section with a 'Call Us Now' button. The network traffic panel on the right shows a list of requests, with the 'Request Cookies' tab selected. The cookies table lists various cookies, including 'ar_debug', 'c_user', 'datr', 'fr', 'ps_n', 'sb', and 'xs'. The 'xs' cookie is highlighted with a red box.

Name	Value	Do...	Path	Exp...	Size	htt...	Sec...	sa...	Part...	Cro...	Pri...
ar_debug	1	.fac...	/	Ses...	9	✓	✓	None		Me...	
c_user	100094391277822	.fac...	/	202...	21	✓	✓	None		Me...	
datr	9JwFzZzEzMytw2myjHPHqkQ	.fac...	/	202...	28	✓	✓	None		Me...	
fr	1FGPRfcEtIghkrHDg.AWdtwRII2...	.fac...	/	202...	122	✓	✓	None		Me...	
ps_n	1	.fac...	/	202...	5	✓	✓	None		Me...	
sb	9JwFzYn5gA7T71LHn6OOpnC...	.fac...	/	202...	26	✓	✓	None		Me...	
xs	34%3A75tSCJEnmTXow%3A2...	.fac...	/	202...	97	✓	✓	None		Me...	

58. Through this Meta Pixel, Mr. Cooper disclosed details about users' interactions with its Website, which allowed Meta to identify individual Customers and link them to any logged-in Facebook accounts. The Meta Pixel also permitted Meta to track Customers' activity on Mr. Cooper's Website. For example, a user seeking to refinance a loan can click on the button labeled "Getting Cash from Equity." After the user clicks on the button, Mr. Cooper would report to Facebook that the user is on a page for "simple-cash-options." If, on the following page, the Customer clicks the option to "Get Cash tap into your home's equity with or without refinancing

1 your first mortgage,” the Meta Pixel historically would send an event to Facebook reporting that
 2 the user is on a page for “loantype=get-cash.” Further, after the user completes a set of questions,
 3 Mr. Cooper reports to Facebook that the user submitted an application and completed registration.
 4

5 *ii. Mr. Cooper’s Installed Google and Microsoft Pixels to Track Customers’ Activity and*
 6 *Share Customers’ Personal and Financial Information.*

7 59. Mr. Cooper also shares Customers’ browsing activities and data with Microsoft and
 8 Google.

9 60. For example, Mr. Cooper discloses users’ status as existing loan customers when
 10 they log in to view their account details. As users authenticate and navigate to pages such as their
 11 loan overview and monthly statements, Mr. Cooper transmits events to third parties that reveal
 12 users’ customer status.
 13

14 61. And when a user successfully logs in to Mr. Cooper’s Website, Mr. Cooper sends
 15 events to Google and Microsoft disclosing that the user has landed on the “Loan Overview” page
 16 at “www.mycooper.com/servicing/overview.” Mr. Cooper also sends a parameter to Google the
 17 user is logged in using the flag “logged_in:Y.” And, if the user navigates to view their statement,
 18 Mr. Cooper reports to Google and Microsoft that the user is on the “Monthly Statements” page.
 19

20 62. If a user navigates to the refinancing pages on Mr. Cooper’s Website, Mr. Cooper
 21 shares with Microsoft and Google: (a) users’ selections from their applications; (b) users’ progress
 22 as they navigate their applications; and (c) the type of information that users are requested by Mr.
 23 Cooper to provide. The data that Mr. Cooper shares about users includes the types of financial
 24 products that users intend to obtain and the specified reason for seeking such financial products.
 25

26 63. For example, if a Customer navigates to the “Getting Cash from Equity” page, the
 27 Website presents the user with options to (i) get cash by tapping into their home’s equity; (ii)
 28 refinance; or (iii) buy or sell a home. Mr. Cooper discloses to Google and Microsoft what option

the user chooses at this step of the application, revealing the specific type of financial product that the user is seeking. For example, if the user clicks to get cash, Mr. Cooper informs Google and Microsoft that the user clicked to get “loantype=get-cash”:

The screenshot displays the Mr. Cooper website's 'Need Cash? We Can Help.' section. It features three main options: 'Get Cash' (highlighted), 'Refinance', and 'Buy or Sell a Home'. The 'Get Cash' option includes a description: 'Tap into your home's equity, with or without refinancing your first mortgage.' Below these options is a detailed disclaimer about second lien home equity loans. The browser's developer tools are open, showing the Network tab. The selected request is from 'https://www.google-analytics.com/gcollect?v=2&tid=6...', and its 'Query String Parameters' are visible, including 'loantype=get-cash' and 'internal_ref=HomePage_Slot_Four'.

64. If the user indicates that they want a loan to get cash, Mr. Cooper inquires why the user is seeking cash and reports the user's answer to Google. For instance, if the user answers that they plan to use the cash to pay off debt, Mr. Cooper reports to Google that the user's “customer_intentions” for obtaining the loan is to “pay_off_debt”:

The screenshot shows the Mr. Cooper website's "How much cash would you like to take out?" calculator. The estimated amount is \$95,000. The browser's developer tools are open, showing the Network tab with a list of requests. The request to <https://www.google-analytics.com/ga/collect?v=2&tid=G-2> is highlighted. The request payload is visible, showing the user's information being sent to Google Analytics, including the user's first name, last name, email, and whether they are an existing customer or not.

15 requests 6.4 kB transferred 880 B resources

65. Mr. Cooper also reports to Google that the user is providing the following categories of information as part of their application to “get cash” with the intent to “pay_off_debt”:

- the amount the user would like to cash out;
- the state in which the user’s property is located;
- the user’s first name, last name, and email;
- whether the user is an existing customer or not; and

1 e. the user's home phone number.

2 66. Once the Customer completes these questions, Mr. Cooper reports to Google and
3 Microsoft that the user submitted their "lead_form."

4
5 67. If the user attempt to obtain a quote online, Mr. Cooper notifies Microsoft that the
6 user selected the option to "Get My Quote Online" and reports that Microsoft seeks to "Pay off
7 Debt." Mr. Cooper also sends an event to Google with a summary of the user's selections, reporting
8 that the user is seeking a loan for "simple_cash_options" and that the user seeks to "pay_off_debt"
9 with the proceeds.
10

11 68. As the next page loads, Mr. Cooper requests details about the user's property such
12 as its location and the property type. Mr. Cooper discloses this information to Microsoft. For
13 example, if the property is located in the state of California, Mr. Cooper notifies Microsoft that the
14 Customer responded "California" on the page where Mr. Cooper asks the user "Where is the
15 property loc[ated]." Additionally, Mr. Cooper discloses that the user is asked "What is the address"
16 on their "rapidrefinance" loan application, and that the user provides the detail, "Single Family
17 Residence." Later, Mr. Cooper discloses that the user responded "Primary Residence" on another
18 page for their "rapid-refinance" loan.
19

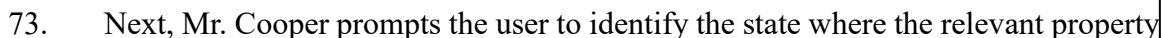
20 69. In the final step, Mr. Cooper requests the user's authorization to perform a soft
21 credit check. If the user selects to provide authorization, Mr. Cooper sends another event to Google,
22 disclosing that the user gives "credit_authorization" for an "Instant Quote – Soft Credit Check"
23 for a "rapid-refinance" loan:
24
25
26
27
28

The screenshot displays the Mr. Cooper website's credit check interface. The page is titled "Ready to check out your best available loan options? This quick credit check gives us the information we need to optimize your quote." It contains two sections for user information: "Fname Lname" and "Sfname Lname". Each section includes a text input for the name, a dropdown for "Last 4 of Your SSN or ITIN", and a date of birth field. Below these are checkboxes for authorizing a soft credit check. A "Continue" button is at the bottom right. The browser's developer console is open, showing a list of network requests. A red box highlights a specific request to "https://www.google-analytics.com/g/collect?v=2&tid=G-2HY4QRV7HT". Another red box highlights the "Query String Parameters" for this request, showing various tracking parameters like "v=2", "tid", "gclid", "cid", "ul", "sr", "uaa", "uab", "uafvl", "uamb", "uam", "uap", "uapv", "uaw", "are", "frm", "pscdl", "ou", "s", "sct", "s", "d", "dr", "dt", "em", "ep.logged_in", "ep.value", "ep.type", "ep.intent", "ep.label", "ep.action", "et", and "tfd".

70. If the user completes an online applications for purchasing or selling a home, Mr. Cooper reports the user's activities to third parties, disclosing (a) some of the users' responses from the application; (b) users' progress as they navigate the application; and (c) the types of information that users are providing Mr. Cooper.

71. As part of the application, the Website asks the user to identify the stage of the home buying/selling process where they currently are: (i) looking at homes and listings; (ii) researching a purchase; (iii) ready to make an offer; (iv) signed a purchase agreement; or (v) selling

72. If the user is in the process of buying a home, Mr. Cooper asks the user whether they are working with a real estate agent and reports that information to Google.



1 is located and discloses the user's response to Microsoft. For example, if the user's property is
2 located in California, Mr. Cooper sends an event to Microsoft reporting that the user responded
3 with "California" in the event.
4

5 74. When the user completes the initial set of questions and submits the application,
6 Mr. Cooper reports that information to Facebook, Microsoft and Google.

7 **D. Mr. Cooper Uses Ambiguous, Disingenuous, and Deceptive Privacy Policies That Fail**
8 **to Sufficiently Disclose or Notify Customers of Defendant's Data Sharing.**

9 *i. Mr. Cooper's Privacy Representations*

10 75. Customers never consented, agreed, authorized, or otherwise permitted Defendant
11 to intercept their Personal and Financial Information or to use or disclose it for marketing and
12 profit purposes. Customers were never provided with any written notice that Defendant disclosed
13 their Personal and Financial Information to Third Parties (who then allowed fourth parties to use
14 it for profit).
15

16 76. Customers relied on Defendant to keep their Personal and Financial Information
17 confidential and securely maintained and to use this information only for the purpose of providing
18 legitimate financial services. Customers relied on Defendant to make only authorized disclosures
19 of this information.
20

21 77. Furthermore, Defendant actively misrepresented it would preserve the security and
22 privacy of Customers' Personal and Financial Information.
23
24
25
26
27
28

78. The contracts that Mr. Cooper has with its Customers include the “Privacy Policy,”²⁶ “Consumer Privacy Notice,”²⁷ and “California Privacy Notice”²⁸ (collectively, “Privacy Contracts”).

79. Mr. Cooper represents that it “take[s] your privacy seriously” and instructs Customers to read the privacy policy for details regarding Mr. Cooper’s privacy practices.²⁹

80. Mr. Cooper’s Privacy Policy reiterates that Mr. Cooper considers customer trust and confidence to be “a high priority”³⁰ and that “[k]eeping financial information is one of our most important responsibilities.”³¹

81. Accordingly, the Privacy Policy is clear that “[o]nly those persons who need it to perform their job responsibilities are authorized to access your information” and that Mr. Cooper “take[s] commercially reasonable precautions to protect your information and limit disclosure by maintaining physical, electronic and procedural safeguards.”³²

82. The Privacy Policy identifies the parties with whom Mr. Cooper may share information, including:

- a. “Within the Mr. Cooper family of companies, . . . [a]ffiliate companies providing financial and other services, such as mortgage lenders, insurance agencies, home security companies, lawn care and pest control and residential homebuilders.”³³

²⁶ *Privacy Policy*, MR. COOPER, <https://www.mrcooper.com/privacy> (last accessed May 12, 2025) (Exhibit A).

²⁷ *Consumer Privacy Notice*, MR. COOPER, https://www.mrcooper.com/reference_documents/apollo_mr_cooper/MrCooper_Privacy_Notice.pdf (last visited May 12, 2022) (Exhibit B).

²⁸ *California Privacy Notice*, MR. COOPER, https://www.mrcooper.com/reference_documents/california_residents.pdf (last visited Mar. 12, 2024) (Exhibit C).

²⁹ *Terms and Conditions*, supra note 8.

³⁰ *Privacy Policy*, Ex. A at 1.

³¹ *Id.* at 2.

³² *Id.*

³³ *Id.*

b. “With Third Party Service Providers, Joint Marketers and As Otherwise Permitted by Law . . . to provide services on our behalf in connection with the servicing of your account or to provide you with opportunities to buy products or services offered by us or jointly with other financial institutions. Consequently, we may disclose some or all of the information that we collect . . . to:

- Companies that perform services on our behalf, such as check and statement printers, data processing companies and vendors who monitor the status of insurance on the property
- Companies with whom we have joint marketing agreements”³⁴

c. “With regulatory authorities and law enforcement officials.”³⁵

d. “To protect against fraud”³⁶

e. “To report activity to credit bureaus”³⁷

f. “To respond to a subpoena”³⁸

g. “To service your account”³⁹

h. “With Other Third Parties” such as “non-affiliated companies or other organizations, including:” “Financial service providers, such as mortgage bankers, securities broker-dealers and insurance agents”; “Non-financial companies, such as retailers, direct marketers, membership clubs and publishers”; “Other companies and organizations, such as non-profit organizations.”⁴⁰

83. The Privacy Policy promises: “For your protection, we require that these companies keep all personal information confidential.”⁴¹

84. The Privacy Policy also notifies customers that “We” (i.e., Mr. Cooper, not any Third Party) “may send ‘cookies’ to your computer primarily to enhance your online experience”

³⁴ *Id.* at 3.

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Id.*

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *Id.* at 3-4.

⁴¹ *Id.* at 3.

as well as other “[t]racking systems” that deliver graphic images on a web page for the purpose of transferring data or letting Mr. Cooper “know whether you received and opened our e-mail.”⁴² Such disclosures never warn Customers that (1) Third Parties like Facebook, Google, or Meta will use cookies or trackers to obtain the confidential Personal and Financial Information that Customers provided to Mr. Cooper; or (2) that Mr. Cooper would share Customers’ Personal and Financial Information with Third Parties to enable Third and Fourth parties to market Third and Fourth-Party products to Plaintiff and the Class that are unrelated to the mortgage services Mr. Cooper offers.

85. The Consumer Privacy Notice recognizes that, under federal law, Customers may limit “sharing for nonaffiliates to market to” them.⁴³ Mr. Cooper’s Consumer Privacy Notice represents:

Federal law also requires us to tell you how we collect, share, and protect your personal information. . . ***The types of personal information we collect and share depend on the product or service you have with us.*** This information can include:

- Social Security number
- Account balances and payment history
- Transaction History
- Income
- Credit history and credit scores⁴⁴

86. But the types of personal information that Mr. Cooper collects and shares does ***not*** depend on the product or service a Customer has with it. Instead, Mr. Cooper indiscriminately collects and shares Customer information without regard to the product or service a Customer has with Mr. Cooper.

87. Mr. Cooper “list[s] the reasons financial companies can share their customers’

⁴² *Privacy Policy*, Ex. A at 5.

⁴³ Consumer Privacy Notice, Ex. B at 2.

⁴⁴ *Id.* (emphasis added).

personal information; the reasons Mr. Cooper chooses to share; and whether you can limit this sharing.”⁴⁵ Those reasons include “our everyday business purposes -- such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus”; “For our marketing purposes -- to offer our products and services to you”; “For joint marketing with other financial companies”; “For our affiliates’ everyday business purposes -- information about your transactions and experiences”; “For our affiliates’ everyday business purposes -- information about your creditworthiness”; “For our affiliates to market to you”; and “For our nonaffiliates to market to you.”⁴⁶

88. The Consumer Privacy Notice defines an Affiliate as “Companies related by common ownership or control. They can be financial and nonfinancial companies.”⁴⁷ Joint marketing is “A formal agreement between nonaffiliated financial companies that together market financial products or services to [Customers].”⁴⁸ Mr. Cooper’s “joint marketing partners include companies such as other banks and insurance companies.”⁴⁹ Certainly, Third Parties like Facebook do not meet either of these definitions. Mr. Cooper finally defines “nonaffiliates,” which are “Companies not related by common ownership or control.”⁵⁰ “They can be financial and nonfinancial companies.”⁵¹ Mr. Cooper identifies the types of “[n]onaffiliates” it can share with as “Financial service providers, such as mortgage bankers, securities broker-dealers and insurance agents &/or agencies” and “Non-Financial companies, such as retailers, direct marketers, membership clubs and publishers; and other companies and organizations, such as nonprofit

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.* at 2.

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ *Id.*

1 organizations.”⁵² It is not clear that the Third Parties at issue fall under this category—Facebook,
2 for example, is a social media company, not an insurance company, retailer, publisher, or nonprofit
3 organization.
4

5 89. In stating that it “can include” its Customers’ Personal and Financial Information,
6 the Consumer Privacy Notice grants Mr. Cooper the sole discretion to determine whether it will
7 share Customers’ information with nonaffiliates. It does not include any information explaining or
8 specifying what information it shares with nonaffiliates or under what conditions and
9 circumstances it may do so. Mr. Cooper thus maintains complete discretion on whether and what
10 to disclose and when it discloses it.
11

12 90. Customers reasonably understand that Mr. Cooper will securely maintain their
13 Personal and Financial Information entrusted to it and protect that information from being shared
14 or utilized by Third Parties (and fourth parties) that have nothing to do with Mr. Cooper or its
15 services. Mr. Cooper’s Consumer Privacy Notice only reinforced this reasonable understanding.
16

17 91. Nevertheless, Mr. Cooper abuses the contractual discretion it reserved wholly for
18 itself and acts in a manner that it knows to be inconsistent with its Customers’ reasonable
19 expectations under its Consumer Privacy Notice.
20

21 92. By always exercising its discretion in its own favor and to the detriment of
22 Customers, Defendant breaches the reasonable expectations of Customers and, in doing so,
23 violates its duty to act in good faith.

24 93. Finally, Mr. Cooper specifically represents to California residents that they have the
25 “right[] to restrict the sharing of personal and financial information with our affiliates . . . and
26 outside companies we do business with. Nothing in this form prohibits the sharing of information
27

28

⁵² *Id.*

1 necessary for us to follow the law, as permitted by law, or to give you the best service on your
2 accounts with us.”⁵³

3
4 94. California consumers like Plaintiff reasonably understand this language to mean
5 that Mr. Cooper will only share their information with its affiliates or outside companies Mr.
6 Cooper does business with as “necessary” to follow the law or to service consumers’ accounts with
7 Mr. Cooper.

8
9 95. In contrast to this reasonable understanding, Mr. Cooper indiscriminately shares
10 Personal and Financial Information with nonaffiliated Third Parties, without Customers’ consent
11 and for Third Party and fourth party marketing purposes that have nothing to do with servicing
12 consumers’ Mr. Cooper accounts.

13 *ii. Third-Parties Further Share the Data and Information Collected from Trackers*
14 *Installed on Mr. Cooper’s Website with Fourth Parties.*

15 96. In addition to using the data for their own purposes, the third parties that obtain
16 Customer data and information from trackers installed on Mr. Cooper’s website further profit from
17 Mr. Cooper’s improper sharing practices by selling Customers’ data to fourth parties.

18
19 97. As one study found, “on average, companies that allow external sharing of [] data
20 assets have data that has been exposed to 42 4th-party domains.”⁵⁴

21 98. Consequently, a fourth party that did not have a tracker directly installed on the Mr.
22 Cooper’s website may obtain and use information collected via third-party trackers to provide
23 direct advertisements to Customers on the fourth party’s platform.

24
25
26 ⁵³ *California Privacy Notice*, Ex. C at 1.

27 ⁵⁴ Adam Gavish, *Your 3rd Party Collaborators Share Your Company’s Data with 4th*
28 *Parties*, DOCONTROL (Feb. 27, 2025), <https://www.docontrol.io/blog/your-3rd-party-collaborators-share-your-company-data-with-4th-parties#:~:text=What%20is%204th%20Party%20Data,side%20effect%20of%20SaaS%20collaboration.>

1 99. One common recipient of Customers' collected data is Facebook.

2 100. For example, Facebook and Google have engaged in practices that allowed for the
3 sharing or accessibility of user data between their platforms.⁵⁵ Because of this, advertisements on
4 Facebook may reflect information collected via a Google tracker, either because of information
5 shared directly or indirectly between the companies.

6 101. A data broker is a company that collects and sells personal information about
7 individuals to other businesses. Data brokers gather consumers' personal information from a
8 variety of sources, and then compile comprehensive profiles they sell for purposes such as targeted
9 advertising, risk assessment, and background checks. Data brokers mass collection and sale of
10 personal information raise significant consumer privacy concerns. The personal data that data
11 brokers collect and sell can be used to harm individuals, for example, by influencing insurance
12 rates, loan denials, and unwanted advertising.

13 102. Both Facebook and Google have a history of sharing the data they receive via
14 analytics technologies with data brokers. For example, when advertisers use Google's real-time
15 bidding system (RTB), RTB lets hundreds of companies bid for ad space on individual consumers
16 based on their Google profile, which can include information such as age, sex, and interests. While
17 only one company will win the auction, hundreds of participating companies receive sensitive
18 information about the potential recipient of the ad—device identifiers and cookies, web browsing
19
20
21
22

23
24 ⁵⁵ See Steven Musil, *Facebook gave tech giants more access to users data than it said*,
25 CBSNEWS (Dec. 19, 2018), <https://www.cbsnews.com/news/facebook-gave-tech-giants-more-access-to-users-data-than-it-said-new-york-times/> (last visited Apr. 24, 2025); Steven Musil,
26 *Facebook acknowledges it shared user data with dozens of companies* (Jul. 1, 2018),
27 <https://www.cnet.com/tech/tech-industry/facebook-acknowledges-it-shared-user-data-with-dozens-of-companies/> (last visited Apr. 24, 2025); Paresh Dave and Katie Paul, *Google secretly gave Facebook perks, data in ad deal* (Dec. 17, 2020),
28 <https://www.reuters.com/article/technology/google-secretly-gave-facebook-perks-data-in-ad-deal-us-states-allege-idUSKBN28Q37G/> (last visited Apr. 24, 2025).

1 and location data, IP addresses, and unique demographic information such as age and gender.
2 Worse, many companies participating in the RTB system are not there to fill ad spaces but instead
3 use RTB to collect users' personal data. Likewise, for users using cell phones or other Android
4 devices that run on a Google operating system, every time they open an app on their Android phone
5 or tablet, Google will timestamp it, and every ad the user is shown will be recorded and associated
6 with their device profile.
7

8 103. Facebook is no better. Facebook has historically collaborated with data brokers to
9 gather consumer data and enhance its user profiles for targeting advertising. Facebook itself acts
10 as a first-party data broker, collecting data from user activities on its platform to offer targeted
11 advertising, which is its primary revenue source. Facebook's data ecosystem extends through
12 external partnerships, allowing Facebook to collect data from user interactions on other websites
13 and apps. Companies that pay for ads on Facebook can then direct users to their websites, which
14 embed trackers that collect information such as IP addresses and device IDs from visitors.
15
16

17 104. Facebook also has a history of sharing its customers data with third parties,
18 including most infamously Cambridge Analytica, who gained access to the data of tens of millions
19 of Facebook users. Facebook has also shared its customers data with "partners," such as Acxiom,
20 Oracle, Epsilon, and Experian. Once this data is shared, neither Facebook or its users have control
21 over this data as it is endlessly sold and resold to data brokers around the world.
22

23 105. The only remedy for users whose information has been shared with Google is to
24 use services such as DeleteMe and CyEx Privacy Shield Pro that go out into the online market
25 place and "delete" users' personal data from data broker rolls. These services, however, cost
26 anywhere from \$100 to \$300 a year on average for consumers to try and regain control over their
27 personal information.
28

106. Facebook and Google both act as data brokers, meaning they collect data, compile it into datasets, and sell it to third parties.⁵⁶ Two other popular data brokers are Acxiom and Oracle Data Cloud (“Oracle”). Facebook and Google have been known to buy information from, and sell information to, such data brokers.⁵⁷

107. Because of this, one company’s tracker (e.g., Google Analytics) may collect information, compile it into a dataset (owned by Google), and act as a data broker to sell it to a third-party (e.g., Facebook), which uses the information to advertise for various parties (like other financial institutions) on its own platform.⁵⁸ Alternatively, one company’s tracker (e.g., Google Analytics) may collect information, compile it into a dataset (owned by Google), and act as a data broker to sell it to a fourth-party advertiser (e.g., another financial institution), which uses the information to advertise for on other platforms (e.g., Facebook).⁵⁹ Or, one company’s tracker (e.g., Google Analytics) may collect information, sell either the raw data or a compiled dataset to a third-party data broker (e.g., Acxiom or Oracle), which third party data broker sells the information to a fourth party (e.g., Facebook), which uses the information for still other parties’ targeted advertising.⁶⁰ In any event, the basic idea and results are the same. Google Analytics tracks and

⁵⁶ See Jessie G Taft, *Facebook and Google Are the New Data Brokers* (Dec. 18, 2018, updated Jan. 5, 2021), <https://dli.tech.cornell.edu/post/facebook-and-google-are-the-new-data-brokers> (last visited Apr. 24, 2025).

⁵⁷ See Kalev Leetaru, *The Data Brokers So Powerful Even Facebook Bought Their Data* (Apr. 05, 2018), <https://www.forbes.com/sites/kalevleetaru/2018/04/05/the-data-brokers-so-powerful-even-facebook-bought-their-data-but-they-got-me-wildly-wrong/> (last visited Apr. 24, 2025).

⁵⁸ See Don Marti, *et. al.*, *Who Shares Your Information With Facebook?* at 16 (Jan. 2024), https://innovation.consumerreports.org/wp-content/uploads/2024/01/CR_Who-Shares-Your-Information-With-Facebook.pdf (explaining how Facebook uses aggregated data from external data brokers to target users on its platform).

⁵⁹ *Id.*

⁶⁰ See Kalev Leetaru, *The Data Brokers So Powerful Even Facebook Bought Their Data* (Apr. 05, 2018), <https://www.forbes.com/sites/kalevleetaru/2018/04/05/the-data-brokers-so-powerful-even-facebook-bought-their-data-but-they-got-me-wildly-wrong/>.

discloses information to fourth parties that use that data and information to advertise a variety of products on a variety of platforms.

108. The information that data brokers like Acxiom and Oracle buy and compile from trackers (like Facebook's and Google's tackers) is inherently sensitive.

E. Mr. Cooper Violated the GLBA, FTC Standards, and Related Regulations

109. As a financial institution, Mr. Cooper is subject to the GLBA. 15 U.S.C. § 6809(3)(A) (a "financial institution" is "any institution the business of which is engaging in financial activities..."). Defendant recognizes this, noting, "If you have a mortgage or an application with us, the information we have about you is protected under federal privacy laws—such as the Gramm Leach Bliley Act and the Fair Credit Reporting Act. It is therefore excluded from state privacy laws, and not covered by the disclosures below."⁶¹

110. Pursuant to the GLBA, "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).

111. The FTC has interpreted Section 5 of the FTC Act, 15 U.S.C. § 45, to include compliance with the GLBA Privacy Rule, 16 C.F.R. § 313.1, *et seq.* The FTC consistently enforces the GLBA Privacy Rule, as failure to comply with the GLBA Privacy Rule is an unfair act or practice prohibited by Section 5 of the FTC Act.⁶²

112. The GLBA Privacy Rule is a regulation that "governs the treatment of nonpublic personal information about consumers by the financial institutions." 16 C.F.R. § 313.1 *et seq.*

⁶¹ *State Consumer Privacy Act Laws – FAQ*, MR. COOPER, <https://www.mrcooper.com/privacy/state> (last accessed May 12, 2025).

⁶² *See How to Comply with the Privacy Rule*, <https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act> ("The FTC may bring enforcement actions for violations of the Privacy Rule.").

1 113. Pursuant to the GLBA Privacy Rule, “[a] financial institution must provide a notice
2 of its privacy policies and practices with respect to both affiliated and nonaffiliated third parties,
3 and allow the consumer to opt out of the disclosure of the consumer’s nonpublic personal
4 information to a nonaffiliated third party if the disclosure is outside of the exceptions.”⁶³ Mr.
5 Cooper consistently fails to do this.

7 114. The GLBA Privacy Rule, defines sensitive information that should not be
8 indiscriminately disclosed:

- 9 (n) (1) Nonpublic personal information means:
- 10 (i) Personally identifiable financial information; and
 - 11 (ii) Any list, description, or other grouping of consumers (and
 - 12 publicly available information pertaining to them) that is derived
 - 13 using any personally identifiable financial information that is not
 - 14 publicly available....
 - 15 (3) Examples of lists—
 - 16 (i) Nonpublic personal information includes any list of individuals’
 - 17 names and street addresses that is derived in whole or in part using
 - 18 personally identifiable financial information (that is not publicly
 - 19 available), such as account numbers....
 - 20 (o) (1) Personally identifiable financial information means any information:
 - 21 (i) A consumer provides to you to obtain a financial product or
 - 22 service from you;
 - 23 (ii) About a consumer resulting from any transaction involving a
 - 24 financial product or service between you and a consumer; or
 - 25 (iii) You otherwise obtain about a consumer in connection with
 - 26 providing a financial product or service to that consumer.
 - 27 (2) Examples—
 - 28 (i) Information included. Personally identifiable financial
 - information:
 - (A) Information a consumer provides to you on an
 - application to obtain a loan, credit card, or other financial
 - product or service;
 - (B) Account balance information, payment history,
 - overdraft history, and credit or debit card purchase
 - information;

⁶³ See FTC, *Financial Privacy Rule*, <https://www.ftc.gov/legal-library/browse/rules/financial-privacy-rule> (last visited August 8, 2024).

- (C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;
- (D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;
- (E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;
- (F) Any information you collect through an Internet “cookie” (an information collecting device from a web server); and
- (G) Information from a consumer report.

16 C.F.R. § 313.3

115. The information that Mr. Cooper disclosed to Third Parties via trackers—including *e.g.*, information revealed in the application process regarding (i) the type and location of the Customer’s property, (ii) the user’s status as Mr. Cooper customer; (iii) the user’s browsing activities, including that the user clicked certain buttons and what URLs or webpages they led to; (iv) the user’s refinancing options and customer selection; (v) the reason the customer is seeking to refinance; (vi) that the user submitted a mortgage and/or refinancing application; (vii) the user’s request for a quote and a summary of the user’s selections; (viii) the type of property at issue; and (ix) the user’s current stage of the homebuying process (which is information Mr. Cooper obtained from the Customer in connection with providing financial products and services)—is “nonpublic personal information” under the GLBA and related regulations. 16 C.F.R. § 313.3.

116. Mr. Cooper has utterly failed to meet its privacy obligations under the GLBA: it has explicitly disclosed Customers’ nonpublic personal information and Personal and Financial Information to Third Parties for marketing and advertisement, including for Third Party and fourth party advertising use.

117. Mr. Cooper fails to meet its notice obligations under the GLBA. “[A] financial

1 institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any
 2 nonpublic personal information, unless such financial institution provides or has provided to the
 3 consumer a notice that complies with section 6803 of this title.” 15 U.S.C.A. § 6802. As outlined
 4 at length above, Mr. Cooper’s Privacy Policies fail to put Customers on notice as required here and
 5 actually promise that Customers’ Personal and Financial Information will not be shared with Third
 6 Parties (and fourth parties) for targeted advertising purposes.

7
 8 118. For example, by not including in its Privacy Policies that it discloses Customers’
 9 Personal and Financial Information to Third Parties for their use in their own advertising and
 10 marketing, the Privacy Policies fail to properly disclose:
 11

- 12 (1) the policies and practices of the institution with respect to disclosing nonpublic
 13 personal information to nonaffiliated third parties . . . including [] the categories
 14 of persons to whom the information is or may be disclosed, other than the
 15 persons to whom the information may be provided [and] the policies and
 16 practices of the institution with respect to disclosing of nonpublic personal
 17 information of persons who have ceased to be customers of the financial
 18 institution . . .
- 19 (2) the categories of nonpublic personal information that are collected by the
 20 financial institution; [and]
- 21 (3) the policies that the institution maintains to protect the confidentiality and
 22 security of nonpublic personal information

23 15. U.S.C.A. § 6803.

24 119. As detailed above, Mr. Cooper also fails to meet its opt out obligations under the
 25 GLBA. The GLBA Privacy Rule requires financial institutions to, for example, “provide an opt
 26 out notice” to Customers, which notice “must state...[t]hat the consumer has the right to opt out
 27 of that disclosure [and] [a] reasonable means by which the consumer may exercise the opt out
 28 right.” 16 C.F.R. § 313.7. Under the GLBA, Mr. Cooper

may not disclose nonpublic personal information to a nonaffiliated third party
 unless—

- (A)[it] clearly and conspicuously discloses to the consumer. . . that such
 information may be disclosed to such third party;

- (B) *the consumer is given the opportunity*, before the time that such information is initially disclosed, *to direct that such information not be disclosed to such third party*; and
- (C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.

15 U.S.C.A. § 6802 (emphasis added).

120. Mr. Cooper fails to meet its opt out obligations because, as outlined above, Mr. Cooper does not clearly and conspicuously disclose to Customers its Disclosure of their Personal and Financial Information to Third Parties.

121. Mr. Cooper further fails to meet its opt out obligations because Customers are not provided an opportunity before disclosure to direct the nondisclosure of their information—as described above, Mr. Cooper instantaneously discloses information when Customers visit its Website.

122. By perpetually disclosing its customers' Personal and Financial Information to third parties without consent, Mr. Cooper failed and continues to fail to meet its obligations under the GLBA, FTC standards, and related regulations, to establish appropriate standards and safeguards relative to Customers' Personal and Financial Information.

F. Plaintiff's Experience

123. Plaintiff Martin Beltran obtained a mortgage with Bank of America in or around 2019. Mr. Cooper bought out the mortgage and so Plaintiff Beltran opened an online account with Mr. Cooper.

124. In 2021, Plaintiff Beltran's mortgage was transferred from Bank of America to Mr. Cooper without him knowing. At that time, Plaintiff Beltran attempted to make a payment to BOA in 2021, but it would not go through. He called BOA to see what was going on, and they directed him to Mr. Cooper. To pay his mortgage, Plaintiff Beltran had to set up an account with Mr. Cooper

1 in the fall of 2021. Plaintiff Beltran has input his SSN, DOB, address, contact information, and
2 more into Mr. Cooper's website.

3
4 125. In or around 2022, Plaintiff Beltran researched refinancing options on Mr. Cooper's
5 website.

6 126. Plaintiff Beltran regularly uses Mr. Cooper's Website to review his account, manage
7 his mortgage, and make payments. He has been using the website anywhere between a few times
8 a month to a few times a week since 2021-2022. He recalls interacting with the following tabs:
9 'calculators', 'refinance', 'buy a home', 'rates', 'apply', 'help', 'get cash from equity', 'sign in',
10 and 'buying or selling a home'.
11

12 127. Plaintiff Beltran is a Facebook user.

13 128. Beginning around the same time Plaintiff Beltran opened an online account with
14 Mr. Cooper, he began receiving advertisements on Facebook and Google regarding refinancing.
15 Over the past 3 years, Plaintiff Beltran has continued to receive regular ads on Facebook and
16 Google regarding the services he reviews on Mr. Cooper's website.
17

18 129. Plaintiff accessed Defendant's Website at Defendant's direction and
19 encouragement.

20 130. Plaintiff relied on Defendant's Website to communicate Personal and Financial
21 Information and did so with the understanding that Mr. Cooper would not share their Personal and
22 Financial Information except as agreed in the Privacy Policies.
23

24 131. At no point did Customers like Plaintiff sign any written authorization permitting
25 Defendant to send their Personal and Financial Information to Third Parties (or fourth parties)
26 uninvolved in providing them with financial or mortgage services.
27

28 132. Plaintiff reasonably expected that their communications with Mr. Cooper were

1 confidential, solely between each Plaintiff and Mr. Cooper, and that, as such, those
2 communications and any Personal and Financial Information submitted would not be transmitted
3 to or intercepted by a third party (or used by a fourth party).
4

5 133. Plaintiff provided their Personal and Financial Information to Defendant and
6 trusted that the information would be safeguarded according to Mr. Cooper's promises and the law.

7 134. Had they been aware of Mr. Cooper's sharing practices, Plaintiff would not have
8 authorized Mr. Cooper to make their Personal or Financial Information available for sale on the
9 resale market.
10

11 135. Plaintiff never intended to let Mr. Cooper benefit from their Personal and Financial
12 Information.

13 136. Through the systematic data sharing process described in this complaint, Plaintiff's
14 interactions with Mr. Cooper's online financial platform were disclosed to third parties, including
15 Facebook. Plaintiff did not consent to those disclosures.
16

17 137. On information and belief, through its use of Third Party trackers on its Website,
18 Defendant disclosed to Third Parties information Plaintiff provided to Mr. Cooper as a financial
19 institution and resulting from a transaction for Plaintiff to obtain or access Defendant's mortgage
20 services, including each Plaintiff's:
21

- 22 a. Existing user or Customer status;
- 23 b. Browsing activities, including the pages and content Plaintiff viewed;
- 24 c. Refinancing options and customer selections;
- 25 d. Reason for refinancing;
- 26 e. Confirmation that their online application was submitted;
- 27 f. Request for a quote and a summary of their selections;
- 28

- g. Property type and location;
- h. Stage of the homebuying process;
- i. c_user cookie to identify a logged-in Facebook account; and
- j. Information collected through an Internet “cookie” (or information collecting device from a web server).

138. By failing to receive the requisite consent, Mr. Cooper breached confidentiality and unlawfully disclosed Plaintiff’s Personal and Financial Information.

139. Plaintiff would not have submitted their information to Mr. Cooper if they had known it would be shared with Third Parties and further sold to fourth parties for purposes of marketing Third and fourth party products.

140. As a result of Mr. Cooper’s Disclosure of Plaintiff’s Personal and Financial Information via the Meta Pixel and other tracking technologies to Third Parties (and fourth parties) without authorization, Plaintiff was harmed in the following ways:

- a. Loss of privacy;
- b. Unauthorized disclosure of his Personal and Financial Information;
- c. Unauthorized access to his Personal and Financial Information by Third Parties;
- d. Mr. Cooper benefited from the use of Plaintiff’s Personal and Financial Information without sharing that benefit with Plaintiff;
- e. Repeated targeted advertisements from Third and fourth parties on social media and other third-party websites, reflecting Plaintiff’s Personal and Financial Information that was improperly disclosed and used;
- f. Lost benefit of his bargain with Mr. Cooper, as Plaintiff did not receive the reasonable privacy and data security protections for which they paid;

- 1 g. Mr. Cooper enriched itself at Plaintiff's expense without sharing the revenue and
2 profit attributable to collecting Plaintiff's Personal and Financial Information
3 without authorization and sharing it with Third Parties (and fourth parties);
4
5 h. Mr. Cooper profited off of disclosing Plaintiff's Personal and Financial Information
6 without authorization and sharing it with Third Parties (and fourth parties) through
7 savings in marketing costs;
8
9 i. Mr. Cooper profited as a result of collecting Plaintiff's Personal and Financial
10 Information without authorization and sharing it with Third Parties (and fourth
11 parties) through its revenues and profits attributable to serving and monetizing
12 advertisements directed to Plaintiff;
13
14 j. Plaintiff lost his ability to keep his Personal and Financial Information private or
15 allow Mr. Cooper to track their data;
16
17 k. Embarrassment, humiliation, frustration, and emotional distress;
18
19 l. Decreased value of Plaintiff's Personal and Financial Information;
20
21 m. Increased risk of future harm resulting from future use and disclosure of his
22 Personal and Financial Information; and
23
24 n. Statutory damages.

TOLLING, CONCEALMENT, AND ESTOPPEL

25 141. The applicable statutes of limitation have been tolled as a result of Mr. Cooper's
26 knowing and active concealment and denial of the facts alleged herein.

27 142. Mr. Cooper seamlessly incorporated trackers into its Website while providing
28 Customers using those platforms with no indication that their Website usage was being tracked
and transmitted to Third Parties. Mr. Cooper knew that its Website incorporated trackers, yet it

1 failed to disclose to Plaintiff and Class Members that their sensitive Personal and Financial
 2 Information would be intercepted, collected, used by, and disclosed to Third Parties.

3
 4 143. Plaintiff and Class Members could not with due diligence have discovered the full
 5 scope of Mr. Cooper's conduct, because there were no disclosures or other indication that they
 6 were interacting with websites employing tracking technology to unauthorizedly disclose their
 7 Personal and Financial Information to unaffiliated Third Parties or that their information would
 8 subsequently be sold to fourth parties for the purpose of marketing third and fourth party products.

9
 10 144. All applicable statutes of limitation have also been tolled by operation of the
 11 discovery rule and the doctrine of continuing tort. Mr. Cooper's illegal interception and disclosure
 12 of Plaintiff's and the Class's Personal and Financial Information has continued unabated. What is
 13 more, Mr. Cooper was under a duty to disclose the nature and significance of its data collection
 14 practices but did not do so. Mr. Cooper is therefore estopped from relying on any statute of
 15 limitations defenses.

16 CLASS ACTION ALLEGATIONS

17
 18 145. Plaintiff brings this nationwide class action on behalf of himself and on behalf of
 19 all other similarly situated persons pursuant to Fed. R. Civ. P. 23.

20 146. Plaintiff seek to represent the following classes:

21
 22 **Nationwide Class:** All individuals in the United States who have had or applied for
 23 mortgage services with Mr. Cooper within the applicable statute of limitations and
 24 whose Personal and Financial Information was disclosed by Defendant to Third
 25 Parties through Defendant's Website's tracking technology without authorization.

26
 27 **California Subclass:** All citizens of California who have had or applied for
 28 mortgage services with Mr. Cooper within the applicable statute of limitations and
 whose Personal and Financial Information was disclosed by Defendant to Third
 Parties through Defendant's Website's tracking technology without authorization.

147. Excluded from the Classes are the following individuals and/or entities: Defendant

1 and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which
2 Defendant has a controlling interest; all individuals who make a timely election to be excluded
3 from this proceeding using the correct protocol for opting out; and all judges assigned to hear any
4 aspect of this litigation, as well as their immediate family members.

5
6 148. Plaintiff reserve the right to modify or amend the definition of the proposed classes
7 before the Court determines whether certification is appropriate.

8
9 149. This action satisfies the numerosity, commonality, typicality, and adequacy
10 requirements under Fed. R. Civ. P. 23(a)(1)-(4).

11 150. Numerosity: Class Members are so numerous and geographically dispersed that
12 joinder of all members is impracticable. Upon information and belief, there likely millions of
13 individuals throughout the United States whose Personal and Financial Information has been
14 improperly used or disclosed by Defendant, and the Classes are identifiable within Defendant's
15 records.

16
17 151. Ascertainability. Class Members are readily identifiable from information in
18 Defendant's possession, custody, and control.

19 152. Commonality and Predominance: Questions of law and fact common to the Classes
20 exist and predominate over any questions affecting only individual Class Members. These include:

- 21
22 a. Whether Defendant disclosed Class Members' Personal and Financial Information to
23 Third Parties;
- 24 b. Whether Class Members consented to Defendant's disclosure of their Personal and
25 Financial Information;
- 26 c. Whether Defendant owed duties to Plaintiff and Class Members to protect their
27 Personal and Financial Information;
- 28

- d. Whether Defendant breached its duty to protect Plaintiff's and Class Members' Personal and Financial Information;
- e. Whether Defendant's disclosure of Plaintiff's and Class Members' Personal and Financial Information to Third Parties violated federal, state and local laws, or industry standards;
- f. Whether Defendant's failure to allow Customers a meaningful opportunity to opt out of sharing with Third Parties violated federal, state and local laws, or industry standards;
- g. Whether Defendant's conduct resulted in or was the actual cause of the disclosure of Plaintiff's and Class Members' Personal and Financial Information;
- h. Whether Defendant's conduct resulted in or was the proximate cause of the disclosure of Plaintiff's and Class Members' Personal and Financial Information;
- i. Whether Defendant has a contractual obligation to protect Plaintiff's and Class Members' Personal and Financial Information and whether it complied with such contractual obligation;
- j. Whether Defendant has a duty of confidence and whether it complied with such obligation;
- k. Whether Defendant's conduct amounted to violations of state consumer protection statutes;
- l. Whether Defendant's conduct amounted to violations of state and federal wiretap statutes;
- m. Whether Defendant's conduct amounted to violations of other California state laws;
- n. Whether Defendant should retain Plaintiff's and Class Members' valuable Personal and

1 Financial Information;

- 2 o. Whether, as a result of Defendant's conduct, Plaintiff and Class Members are entitled
3 to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such
4 relief.
5

6 153. Defendant has engaged in a common course of conduct toward Plaintiff and the
7 Class Members, in that the Plaintiff's and Class Members' data was stored on the same computer
8 system and unlawfully disclosed and accessed in the same way. As set forth above, the common
9 issues arising from Defendant's conduct affecting Class Members predominate over any
10 individualized issues. Adjudication of these common issues in a single action has important and
11 desirable advantages of judicial economy.
12

13 154. Typicality: Plaintiff's claims are typical of those of other Class Members because
14 all had their Personal and Financial Information compromised as a result of Defendant's use and
15 incorporation of Meta Pixel, Google Pixel, Microsoft Pixel, and other tracking technology.
16

17 155. Policies Generally Applicable to the Classes: This class action is also appropriate
18 for certification because Defendant has acted or refused to act on grounds generally applicable to
19 the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards
20 of conduct toward the Class Members and making final injunctive relief appropriate with respect
21 to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class
22 Members uniformly, and Plaintiff's challenge of these policies hinges on Defendant's conduct with
23 respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.
24

25 156. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of
26 the Class Members in that Plaintiff have no disabling conflicts of interest that would be
27 antagonistic to those of the other Class Members. Plaintiff seek no relief that is antagonistic or
28

1 adverse to the Class Members and the infringement of the rights and the damages Plaintiff have
2 suffered is typical of other Class Members. Plaintiff have also retained counsel experienced in
3 complex class action litigation, and Plaintiff intends to prosecute this action vigorously.
4

5 157. Superiority and Manageability: Class litigation is an appropriate method for fair
6 and efficient adjudication of the claims involved. Class action treatment is superior to all other
7 available methods for the fair and efficient adjudication of the controversy alleged herein; it will
8 permit a large number of Class Members to prosecute their common claims in a single forum
9 simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and
10 expense that hundreds of individual actions would require. Class action treatment will permit the
11 adjudication of relatively modest claims by certain Class Members, who could not individually
12 afford to litigate a complex claim against large corporations, like Defendant. Further, even for
13 those Class Members who could afford to litigate such a claim, it would still be economically
14 impractical and impose a burden on the courts.
15
16

17 158. The nature of this action and the nature of laws available to Plaintiff and Class
18 Members make the use of the class action device a particularly efficient and appropriate procedure
19 to afford relief to Plaintiff and Class Members for the wrongs alleged. If the class action device
20 were not used, Defendant would necessarily gain an unconscionable advantage because it would
21 be able to exploit and overwhelm the limited resources of each individual Class Member with
22 superior financial and legal resources. Moreover, the costs of individual suits could unreasonably
23 consume the amounts that would be recovered, whereas proof of a common course of conduct to
24 which Plaintiff were exposed is representative of that experienced by the Classes and will establish
25 the right of each Class Member to recover on the cause of action alleged. Finally, individual actions
26 would create a risk of inconsistent results and would be unnecessary and duplicative of this
27
28

1 litigation.

2 159. The litigation of the claims brought herein is manageable. Defendant's uniform
3 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class
4 Members demonstrates that there would be no significant manageability problems with
5 prosecuting this lawsuit as a class action.
6

7 160. Adequate notice can be given to Class Members directly using information
8 maintained in Defendant's records.
9

10 161. Unless a Class-wide injunction is issued, Defendant may continue in its unlawful
11 use and disclosure and failure to properly secure the Personal and Financial Information of Plaintiff
12 and the Class Members, Defendant may continue to refuse to provide proper notification to and
13 obtain proper consent from Class Members, and Defendant may continue to act unlawfully as set
14 forth in this Complaint.
15

16 162. Moreover, Defendant has acted or refused to act on grounds generally applicable to
17 the Classes, and, accordingly, final injunctive or corresponding declaratory relief regarding the
18 whole of the Classes is appropriate.

19 163. Likewise, particular issues are appropriate for certification because such claims
20 present only particular, common issues, the resolution of which would advance the disposition of
21 this matter and the parties' interests therein. Such particular issues include, but are not limited to
22 the following:
23

- 24 a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due
25 care in collecting, storing, using, and safeguarding their Personal and Financial
26 Information;
27
28 b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise

- 1 due care in collecting, storing, using, and safeguarding their Personal and Financial
 2 Information;
- 3
- 4 c. Whether Defendant failed to comply with its own policies and applicable laws,
 5 regulations, and industry standards relating to the disclosure of customer information;
- 6 d. Whether Defendant was negligent and/or negligent *per se*;
- 7 e. Whether an implied contract existed between Defendant on the one hand, and Plaintiff
 8 and Class Members on the other, and the terms of that contract;
- 9 f. Whether Defendant breached the contract;
- 10 g. In the alternate, whether Defendant was unjustly enriched;
- 11 h. Whether Defendant adequately and accurately informed Plaintiff and Class Members
 12 that their Personal and Financial Information had been used and disclosed to Third
 13 Parties and used for Third Party and fourth parties' benefit;
- 14 i. Whether Defendant failed to implement and maintain reasonable security procedures
 15 and practices;
- 16 j. Whether Defendant invaded Plaintiff and the Class Members' privacy;
- 17 k. Whether Defendant breached its implied duty of confidentiality; and,
- 18 l. Whether Plaintiff and the Class Members are entitled to actual, consequential, and/or
 19 nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.
 20
 21
 22

23 **COUNT I**
 24 **NEGLIGENCE**

25 **(On Behalf of Plaintiff, the Nationwide Class, and the California Subclass)**

26 164. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

27 165. Plaintiff and Class Members submitted sensitive nonpublic personal information,
 28 including Personal and Financial Information, when accessing Mr. Cooper's Website.

1 166. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care
2 in handling and using Plaintiff's and Class Members' Personal and Financial Information in its
3 care and custody, including implementing industry-standard privacy procedures sufficient to
4 reasonably protect the information from disclosure and unauthorized transmittal and use of
5 Personal and Financial Information that occurred.
6

7 167. Defendant's duties to keep the nonpublic personal information, including Personal
8 and Financial Information, confidential also arose under the GLBA, which imposes "an affirmative
9 and continuing obligation to respect the privacy of its customers and to protect the security and
10 confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).
11

12 168. Defendant's duties to keep the nonpublic personal information, including Personal
13 and Financial Information, confidential also arose under Section 5 of the Federal Trade
14 Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting
15 commerce," including the unfair practice of failing to keep the nonpublic personal information
16 confidential.
17

18 169. Plaintiff and Class Members are within the class of persons that these statutes and
19 rules were designed to protect.
20

21 170. Defendant acted with wanton and reckless disregard for the privacy and
22 confidentiality of Plaintiff's and Class Members' Personal and Financial Information by disclosing
23 and providing access to this information to Third Parties for the financial benefit of Third Parties
24 (and fourth parties) and Defendant.

25 171. Defendant owed these duties to Plaintiff and Class Members because they are
26 members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew
27 or should have known would suffer injury-in-fact from Defendant's disclosure of their Personal
28

1 and Financial Information to benefit Third Parties (and fourth parties) and Defendant. Defendant
2 actively sought and obtained Plaintiff's and Class Members' Personal and Financial Information.
3
4 And Defendant knew or should have known that by integrating tracking technology on its Website
5 that Plaintiff's and Class Members' nonpublic personal information, including Personal and
6 Financial Information, would be disclosed to the Third Parties (and used by the fourth parties).

7 172. Personal and Financial Information is highly valuable, and Defendant knew, or
8 should have known, the harm that would be inflicted on Plaintiff and Class Members by disclosing
9 their Personal and Financial Information to Third Parties. This disclosure was of benefit to the
10 Third Parties (and fourth parties) and Defendant by way of data harvesting, advertising, and
11 increased sales.
12

13 173. Defendant breached its duties by failing to exercise reasonable care in supervising
14 its agents, contractors, vendors, and suppliers in the handling and securing of Personal and
15 Financial Information of Plaintiff and Class Members. This failure actually and proximately
16 caused Plaintiff's and Class Members' injuries.
17

18 174. As a direct, proximate, and traceable result of Defendant's negligence and/or
19 negligent supervision, Plaintiff and Class Members have suffered or imminently will suffer injury
20 and damages, including monetary damages, inappropriate advertisements and use of their Personal
21 and Financial Information for advertising purposes, and increased risk of future harm,
22 embarrassment, humiliation, frustration, and emotional distress.
23

24 175. Defendant's negligence and breach of its common-law duties to exercise reasonable
25 care directly and proximately caused Plaintiff's and Class Members' actual, tangible, injury-in-
26 fact and damages, including, without limitation: the unauthorized access of their Personal and
27 Financial Information by Third Parties (and fourth parties); improper disclosure of their Personal
28

1 and Financial Information; receipt of targeted advertisements reflecting private financial
2 information; lost benefit of their bargain; lost value of their Personal and Financial Information
3 and diminution in value; embarrassment, humiliation, frustration, and emotional distress; lost time
4 and money incurred to mitigate and remediate the effects of use of their information, as to targeted
5 advertisements that resulted from and were caused by Defendant's negligence; value to Plaintiff
6 and the Class Members of surrendering their choices to keep their Personal and Financial
7 Information private and allowing Defendant to track their data; increased risk of future harm
8 resulting from future use and disclosure of Plaintiff's and the Class Members' Personal and
9 Financial Information; and other injuries and damages as set forth herein. These injuries are
10 ongoing, imminent, immediate, and continuing.

13 176. Defendant's negligence directly and proximately caused the unauthorized access
14 and disclosure of Plaintiff's and Class Members' Personal and Financial Information, and as a
15 result, Plaintiff and Class Members have suffered and will continue to suffer damages as a result
16 of Defendant's conduct. Plaintiff and Class Members seek actual and compensatory damages, and
17 all other relief they may be entitled to as a proximate result of Defendant's negligence.

19 177. Plaintiff and Class Members seek to recover the value of the unauthorized access
20 to their Personal and Financial Information resulting from Defendant's wrongful conduct. This
21 measure of damages is analogous to the remedies for unauthorized use of intellectual property.
22 Like a technology covered by a trade secret or patent, use or access to a person's personal
23 information is non-rivalrous—the unauthorized use by another does not diminish the rights-
24 holder's ability to practice the patented invention or use the trade-secret protected technology.
25 Nevertheless, a Plaintiff may generally recover the reasonable use value of the intellectual
26 property—i.e., a “reasonable royalty” from an infringer. This is true even though the infringer's
27
28

1 use did not interfere with the owner’s own use (as in the case of a non-practicing patentee) and
 2 even though the owner would not have otherwise licensed such intellectual property to the
 3 infringer. A similar royalty or license measure of damages is appropriate here under common law
 4 damages principles authorizing recovery of rental or use value. This measure is appropriate
 5 because (a) Plaintiff and Class Members have a protectible property interest in their Personal and
 6 Financial Information; (b) the minimum damages measure for the unauthorized use of personal
 7 property is its rental value; and (c) rental value is established with reference to market value, i.e.,
 8 evidence regarding the value of similar transactions
 9
 10

11 178. Plaintiff and Class Members are also entitled to punitive damages resulting from
 12 the malicious, willful, and intentional nature of Defendant’s actions, directed at injuring Plaintiff
 13 and Class Members in conscious disregard of their rights. Such damages are needed to deter
 14 Defendant from engaging in such conduct in the future.
 15

16 **COUNT II**
 17 **VIOLATION OF THE COMPREHENSIVE COMPUTER DATA ACCESS**
 18 **AND FRAUD ACT, CAL. PENAL CODE § 502**
 19 **(On Behalf of Plaintiff and the California Subclass)**
 20

21 179. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.
 22

23 180. The California Legislature enacted the Comprehensive Computer Data Access and
 24 Fraud Act, Cal. Penal Code § 502 to “expand the degree of protection afforded to individuals,
 25 businesses, and governmental agencies from tampering, interference, damage, and unauthorized
 26 access to lawfully created computer data and computer systems,” and finding and declaring “that
 27 the proliferation of computer technology has resulted in a concomitant proliferation of computer
 28 crime and other forms of unauthorized access to computers, computer systems, and computer
 data.” Cal. Penal Code § 502(a).

181. In enacting the CDAFA, the Legislature further found and declared “that protection

1 of the integrity of all types and forms of lawfully created computers, computer systems, and
2 computer data is vital to the protection of the privacy of individuals as well as to the well-being of
3 financial institutions, business concerns, governmental agencies, and others within this state that
4 lawfully utilize those computers, computer systems, and data.” Cal. Penal Code § 502(a).
5

6 182. Plaintiff’s and the Class Members’ devices on which they accessed Defendant’s
7 Online Platforms and Websites, including their computers, smart phones, and tablets, constitute
8 computers or “computer systems” within the meaning of CDAFA. Cal. Penal Code § 502(b)(5).
9

10 183. By conduct complained of in the preceding paragraphs, Defendant violated Section
11 502(c)(1)(B) of CDAFA by knowingly accessing without permission Plaintiff’s and Class
12 Members’ devices in order to wrongfully obtain and use their personal data, including their
13 Personal and Financial Information, in violation of Plaintiff’s and Class Members’ reasonable
14 expectations of privacy in their devices and data.
15

16 184. Defendant violated Cal. Penal Code § 502(c)(2) by knowingly and without
17 permission accessing, taking, copying, and using Plaintiff’s and the Class Members’ Personal and
18 Financial Information.

19 185. Defendant used Plaintiff’s and Class Members’ data as part of a scheme to defraud
20 them and wrongfully obtain their data and other economic benefits. Specifically, Defendant
21 intentionally concealed from Plaintiff and Class Members that Defendant had secretly installed
22 tracking pixels on its Online Platforms that surreptitiously shared Personal and Financial
23 Information with third party advertising companies like Facebook. Had Plaintiff and Class
24 Members been aware of this practice, they would not have used Defendant’s Website and Online
25 Platforms.
26

27 186. The computers and mobile devices that Plaintiff and Class Members used when
28

1 accessing Defendant's Website all have and operate "computer services" within the meaning of
 2 CDAFA. Defendant violated § 502(c) of the CDAFA by knowingly and without permission
 3 accessing and using those devices and computer services, and/or causing them to be accessed and
 4 used, *inter alia*, in connection with the Third Parties' (and fourth parties') wrongful use of such
 5 data.
 6

7 187. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any
 8 set of computer instructions that are designed to . . . record, or transmit information within a
 9 computer, computer system, or computer network without the intent or permission of the owner of
 10 the information."
 11

12 188. Defendant violated § 502(c)(8) by knowingly and without permission introducing
 13 a computer contaminant via trackers embedded into the Online Platforms which intercepted
 14 Plaintiff's and the Class Members' private and sensitive financial information.
 15

16 189. Defendant's violation of the CDAFA caused Plaintiff and Class Members, at
 17 minimum, the following damages:

- 18 a. Sensitive and confidential information that Plaintiff and Class Members intended to
 19 remain private is no longer private;
- 20 b. Defendant eroded the essential confidential nature of their relationship;
- 21 c. Defendant took something of value from Plaintiff and Class Members and derived
 22 benefit therefrom without Plaintiff's and Class Members' knowledge or informed
 23 consent and without sharing the benefit of such value;
- 24 d. Plaintiff and Class Members did not get the full value of the financial services for which
 25 they paid, which included Defendant's duty to maintain confidentiality; and
 26
- 27 e. Defendant's actions diminished the value of Plaintiff's and Class Members' Private
 28

Information.

190. Plaintiff and the Class Members seek compensatory damages in accordance with Cal. Penal Code § 502(e)(1), in an amount to be proved at trial, and injunctive or other equitable relief; as well as punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) as Defendant's violations were willful and, upon information and belief, Defendant is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294; and reasonable attorney's fees under § 502(e)(2).

191. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT III
VIOLATION OF CALIFORNIA'S CONSUMER PROTECTION LAW ("UCL"), CAL.
BUS. & PROF. CODE §§ 17200, *et seq.*
(On Behalf of Plaintiff and the California subclass)

192. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

193. Plaintiff and Defendant are each a "person" under Cal. Bus. & Prof. Code § 17201.

194. The California Business and Professions Code §§ 17201, *et seq.* prohibits acts of unfair competition, which includes unlawful business practices.

195. Defendant's business acts and practices are "unlawful" under the Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et seq.* (the "UCL") because, as alleged above, Defendant violated California common law, and other statutes and causes of action alleged herein.

196. Defendant engaged in unlawful acts and practices by imbedding the Pixel on its Websites, which tracks, records, and transmits Plaintiff's and Class Members' Personal and Financial Information they disclose to Defendant in confidence its Website to Third Parties without Plaintiff's and Class Members' knowledge and/or consent, in violation of the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; the Comprehensive Computer Data Access and

1 Fraud Act, Cal. Penal Code § 502; and by representing that their services have characteristics, uses,
2 or benefits that they do not have in violation of Civil Code § 1770.

3
4 197. When using Defendant's Website and services, Plaintiff and Class Members relied
5 on Defendant's status as a trusted financial institution.

6 198. Inconsistent with its role as a financial service provider, Defendant disclosed
7 Plaintiff's and Class Members' Personal and Financial Information to Third Parties without their
8 consent and for marketing purposes. Thus, Defendant represented that its services have
9 characteristics, uses, or benefits that they do not have and represented that its services are of a
10 particular standard, quality, or grade when they were not, in violation of Cal. Civil Code § 1770.

11
12 199. Plaintiff and Class Members were reasonable to assume, and did assume, that
13 Defendant would take appropriate measures to keep their Personal and Financial Information
14 secure and not share it with Third Parties or allow Third Parties (and fourth parties) to use it without
15 their express consent. Defendant also had a duty to disclose that it was sharing their Customers'
16 Personal and Financial Information with Third Parties. However, Defendant did not disclose at any
17 time that it was sharing this Personal and Financial Information with Third Parties via tracking
18 technologies or that Third Parties (and fourth parties) were using their Personal and Financial
19 Information.
20

21
22 200. Had Plaintiff and Class Members known that Defendant would intercept, collect,
23 and transmit their Personal and Financial Information to Third Parties, Plaintiff and the Class
24 Members would not have used Defendant's services.

25 201. Plaintiff and Class Members have a property interest in their Personal and Financial
26 Information. By surreptitiously collecting and otherwise misusing Plaintiff's and Class Members'
27 Personal and Financial Information, Defendant has taken property from Plaintiff and Class
28

Members without providing just (or indeed any) compensation.

202. By deceptively collecting, using, and sharing Plaintiff's and Class Members' Personal and Financial Information with Third Parties for Third Party (and fourth parties) use, Defendant has taken money or property from Plaintiff and Class Members. Accordingly, Plaintiff seek restitution on behalf of themselves and the Class.

203. Defendant's business acts and practices also meet the unfairness prong of the UCL according to all three theories of unfairness.

204. First, Defendant's business acts and practices are "unfair" under the UCL pursuant to the three-part test articulated in *Camacho v. Automobile Club of Southern California* (2006) 142 Cal. App. 4th 1394, 1403: (a) Plaintiff and Class Members suffered substantial injury due to Defendant's Disclosure of their Personal and Financial Information; (b) Defendant's disclosure of Plaintiff's and Class Members' Personal and Financial Information provides no benefit to Customers, let alone any countervailing benefit that could justify Defendant's Disclosure of Personal and Financial Information without consent for marketing purposes or other pecuniary gain; and (c) Plaintiff and Class Members could not have readily avoided this injury because they had no way of knowing that Defendant was implementing tracking technology.

205. Second, Defendant's business acts and practices are "unfair" under the UCL because they are "immoral, unethical, oppressive, unscrupulous, or substantially injurious" to Plaintiff and Class Members, and "the utility of [Defendant's] conduct," if any, does not "outweigh the gravity of the harm" to Plaintiff and Class Members. *Drum v. San Fernando Valley Bar Ass'n*, (2010) 182 Cal. App. 4th 247, 257. Defendant secretly collected, disclosed, and otherwise misused Plaintiff's and Class Members' Personal and Financial Information by bartering it to Third Parties in return for marketing and profit. This surreptitious, willful, and undisclosed conduct is immoral,

1 unethical, oppressive, unscrupulous, and substantially injurious. Moreover, no benefit inheres in
2 this conduct, the gravity of which is significant.

3
4 206. Third, Defendant's business acts and practices are "unfair" under the UCL because
5 they run afoul of "specific constitutional, statutory, or regulatory provisions." *Drum*, 182 Cal. App.
6 4th at 256 (internal quotation marks and citations omitted). California has a strong public policy
7 of protecting consumers' privacy interests, including consumers' personal data, as codified in
8 California's Constitution in Article I, section 1; the California Invasion of Privacy Act, Cal. Penal
9 Code §§ 630, *et seq.*; and the CDAFA, Cal. Penal Code § 502, among other statutes.

10
11 207. Defendant violated this public policy by, among other things, surreptitiously
12 collecting, disclosing, and otherwise exploiting Plaintiff's and Class Members' Personal and
13 Financial Information by sharing that information with Third Parties via tracking technologies
14 without Plaintiff's and/or Class Members' consent.

15
16 208. Had Plaintiff and Class Members known Defendant would intercept, collect, and
17 transmit their Personal and Financial Information to Facebook and other Third Parties, Plaintiff
18 and Class Members would not have used Defendant's services.

19
20 209. Plaintiff and Class Members were reasonable to assume, and did assume, that
21 Defendant would take appropriate measures to keep their Personal and Financial Information
22 secure and not share it with Third Parties without their express consent. Defendant was in sole
23 possession of and had a duty to disclose the material information that Plaintiff's and Class
24 Members' Personal and Financial Information would be shared with Third Parties via trackers.
25 Defendant did not disclose at any time that they were sharing this Personal and Financial
26 Information with Third Parties via trackers.

27
28 210. Plaintiff and Class Members have a property interest in their Personal and Financial

Information. By surreptitiously collecting and otherwise misusing Plaintiff's and Class Members' Personal and Financial Information, Defendant has taken property from Plaintiff and Class Members without providing just (or indeed any) compensation.

211. Plaintiff and Class Members have lost money and property due to Defendant's conduct in violation of the UCL. Personal and Financial Information such as that which Defendant collected and transmitted to Third Parties has objective monetary value. Companies are willing to pay for Personal and Financial Information, like the information Defendant unlawfully collected and transmitted to Third Parties. For example, in 2015 Pfizer annually paid approximately \$12 million to purchase similarly sensitive information on health data, from various sources.⁶⁴ Data shows that email addresses alone are worth around \$89 apiece to companies.⁶⁵ And estimates show "the annual value of your data if you live in the US is at least \$700" per user.⁶⁶

212. By deceptively collecting, using, and sharing Plaintiff's and Class Members' Personal and Financial Information with Third Parties, and by allowing Third Parties (and fourth parties) to use their Personal and Financial Information, Defendant has taken money and/or property from Plaintiff and Class Members. Accordingly, Plaintiff seek restitution on behalf of themselves and the Class.

213. As a direct and proximate result of Defendant's unfair and unlawful methods and practices of competition, Plaintiff and Class Members suffered actual damages, including, but not limited to, the loss of the value of their Personal and Financial Information.

⁶⁴ SciAm, *How Data Brokers Make Money Off Your Medical Records*, <https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/> (last visited Sept. 8, 2025).

⁶⁵ *What Are Data Brokers and What's Your Data Worth?*, WebFx, <https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/> (last visited Sept. 8, 2025).

⁶⁶ *Id.*

214. As a direct and proximate result of its unfair and unlawful business practices, Defendant has each been unjustly enriched and should be required to make restitution to Plaintiff and Class Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code, disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices, declaratory relief, attorney fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

COUNT IV
VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT,
Cal. Civ. Code § 1798.100, *et seq.*
(On Behalf of Plaintiff and the California subclass)

215. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

216. The CCPA grants consumers rights, including the right to know what personal information is being collected about them and whether that information is sold or disclosed and to whom, the right to prohibit the sale of their personal information, the right to request deletion of their personal information, and the right to nondiscrimination in service and price when they exercise privacy rights. Cal. Civ. Code § 1798.100, *et seq.*

217. The CCPA dictates specifically that “[a] third party shall not sell or share personal information about a consumer that has been sold to, or shared with, the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out.” Cal. Civ. Code § 1798.115 (emphasis added).

218. Defendant collected Plaintiff’s and Class Members Personal and Financial Information, including their personal information, with the purpose of providing financial services in the course of and as part of its business in California.

219. Disclosing Plaintiff’s and Class Members’ Personal and Financial Information to Third Parties was not reasonably necessary or proportionate to perform the reasonably expected

1 financial services that they applied for or received.

2 220. By collecting, using, and selling Plaintiff's and Class Members' personal
3 information and location data to Third Parties for Third Party (and fourth party) use, all without
4 providing consumers with notice, Defendant violated the CCPA.

5 221. By failing to inform Customers like Plaintiff and Class Members of the personal
6 information collected about them and the Third Parties with whom that personal information was
7 shared, and the Third Parties' (and fourth parties') use of that personal information, Defendant
8 violated the CCPA.

9 222. By failing to abide by Customers' requests to delete collected personal information,
10 Defendant violated the CCPA.

11 223. Pursuant to Cal. Civ. Code § 1798.150(b), Plaintiff sent Defendant notice of his
12 CCPA claims shortly after the date of this filing. To date, Defendant has failed to cure the CCPA
13 violation. Plaintiff seeks claims for monetary relief, including statutory and actual damages under
14 the CCPA.

15 224. As a result of Defendant's reckless violations, Plaintiff are entitled to actual
16 damages, statutory damages, and attorneys' fees and costs. Cal. Civ. Code § 1798.150.

17
18 **COUNT V**
19 **BREACH OF EXPRESS AND IMPLIED CONTRACT**
20 **(On Behalf of Plaintiff, the Nationwide Class, and the California Subclass)**

21 225. Plaintiff re-alleges and incorporates the preceding paragraphs as if fully set forth
22 herein.

23 226. Plaintiff and Class Members also entered into an express and implied contract with
24 Mr. Cooper when they obtained financial services from Mr. Cooper, or otherwise provided
25 nonpublic personal information, including Personal and Financial Information, to Mr. Cooper.
26
27
28

1 227. As part of these transactions, Mr. Cooper explicitly and implicitly agreed to
2 safeguard and protect Plaintiff's and Class Members' Personal and Financial Information. Included
3 in these promises are those Mr. Cooper made in its Privacy Contracts outlined above.
4

5 228. Plaintiff and Class Members entered into express and implied contracts with the
6 reasonable expectation (based on Mr. Cooper's own express and implied promises) that Mr.
7 Cooper would keep their nonpublic personal information, including Personal and Financial
8 Information, confidential. Plaintiff and Class Members believed that Mr. Cooper would use part
9 of the monies paid to Mr. Cooper under the express and implied contracts to keep their nonpublic
10 personal information, including Personal and Financial Information, confidential.
11

12 229. Plaintiff and Class Members would not have provided and entrusted their nonpublic
13 personal information, including Personal and Financial Information, or would have paid less for
14 Mr. Cooper's services in the absence of the express and implied contract or implied terms between
15 them and Mr. Cooper. The safeguarding of the nonpublic personal information, including Personal
16 and Financial Information, of Plaintiff and class members was critical to realize the intent of the
17 parties.
18

19 230. As extensively detailed above, Mr. Cooper breached its express and implied
20 contracts with Plaintiff and class members to protect their nonpublic personal information,
21 including Personal and Financial Information, when it disclosed that information to Third Parties.
22

23 231. As a direct and proximate result of Mr. Cooper's breach of express and implied
24 contract, Plaintiff and Class Members sustained actual losses and damages as described in detail
25 above.
26

27 **COUNT VI**
28 **UNJUST ENRICHMENT (AS ALTERNATIVE TO CONTRACT CLAIMS)**
 (On Behalf of Plaintiff, the Nationwide Class, and the California Subclass)

1 232. Plaintiff re-alleges and incorporates the preceding paragraphs as if fully set forth
2 herein.

3
4 233. Plaintiff and Class Members have an interest, both equitable and legal and financial,
5 in their Personal and Financial Information, that was conferred upon, collected by, and maintained
6 by Defendant and that was ultimately disclosed without their consent.

7 234. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the
8 form of valuable, sensitive, personal, and financial information—Personal and Financial
9 Information—that Defendant collected from Plaintiff and Class Members under the guise of
10 keeping this information private. Defendant collected, used, and disclosed this information for its
11 own gain, for marketing purposes, and for sale or trade with Third Parties. Defendant did not share
12 this benefit with Plaintiff and Class Members.
13

14 235. Plaintiff and Class Members would not have used Defendant's services, or would
15 have paid less for those services, if they had known that Defendant would collect, use, and disclose
16 their Personal and Financial Information to Third Parties or allow Third Parties (and fourth parties)
17 to use their Personal and Financial Information.
18

19 236. Defendant appreciated or had knowledge of the benefits conferred upon it by
20 Plaintiff and Class Members.
21

22 237. The benefits that Defendant derived from Plaintiff and Class Members rightly
23 belong to Plaintiff and Class Members themselves. Under unjust enrichment principles, it would
24 be inequitable for Defendant to retain the profit and/or other benefits it derived from the unfair and
25 unconscionable methods, acts, and trade practices alleged in this Complaint.
26

27 238. Defendant continues to benefit and profit from its retention and use of Plaintiff's
28 and Class Members' Personal and Financial Information, while its value to Plaintiff and Class

1 Members has been diminished.

2 239. Plaintiff pleads this claim separately as well as in the alternative to claims for
3 damages under Fed. R. Civ. P. 8(a)(3), because if the Court dismisses Plaintiff's claims for damages
4 or enters judgment on them in favor of the Defendant, Plaintiff's will have no adequate legal
5 remedy. Plaintiff make the following allegations in this paragraph only hypothetically and as an
6 alternative to any contrary allegations in her other causes of action, in the event that such causes
7 of action do not succeed. Plaintiff and the Class Members may be unable to obtain monetary,
8 declaratory and/or injunctive relief directly under other causes of action, and, if so, will lack an
9 adequate remedy at law.
10

11 240. Defendant should be compelled to disgorge into a common fund for the benefit of
12 Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of the
13 conduct and the unauthorized Disclosure alleged herein
14

15
16 **COUNT VII**
17 **BREACH OF CONFIDENCE**
18 **(On Behalf of Plaintiff, the Nationwide Class, and the California Subclass)**

19 241. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

20 242. At all times during Plaintiff's and Class Members' interactions with Mr. Cooper,
21 Mr. Cooper was fully aware of the confidential and sensitive nature of Plaintiff's and Class
22 Members' Personal and Financial Information.

23 243. As alleged herein and above, Mr. Cooper's relationship with Plaintiff and Class
24 Members was governed by terms and expectations that Plaintiff's and Class Members' Personal
25 and Financial Information, would be collected, stored, and protected in confidence, and would not
26 be disclosed to Third Parties, or used by Third Parties (and fourth parties) without notice and
27 consent.
28

1 244. Plaintiff and Class Members provided Mr. Cooper with their Personal and Financial
2 Information, with the explicit and implicit understandings that Mr. Cooper would protect and not
3 permit that information to be disseminated to and used by unaffiliated Third Parties (and fourth
4 parties) without notice, consent, and sufficient opportunity to opt out.

5
6 245. Mr. Cooper voluntarily received in confidence Plaintiff's and Class Members'
7 Personal and Financial Information, with the understanding and affirmative representation to
8 Customers that the information would not be disclosed or disseminated to unaffiliated Third Parties
9 for Third Parties' (and fourth parties') marketing purposes.

10
11 246. Mr. Cooper disclosed Plaintiff's and Class Members' Personal and Financial
12 Information, without notice, without express permission, and without opportunity to opt out.

13 247. But for Mr. Cooper's Disclosure of Plaintiff's and Class Members' Personal and
14 Financial Information, in violation of the parties' understanding of confidence, their Personal and
15 Financial Information would not have been disclosed to Third Parties, or used for Third Party (and
16 fourth party) marketing and profit, without their consent.

17
18 248. The injury and harm Plaintiff and Class Members suffered was the reasonably
19 foreseeable result of Mr. Cooper's nonconsensual disclosure of Plaintiff's and Class Members'
20 Personal and Financial Information. Mr. Cooper knew it was disclosing Plaintiff's and Class
21 Members' Personal and Financial Information to Third Parties, for Third Party (and fourth party)
22 use, without their consent.

23
24 249. As a direct and proximate result of Mr. Cooper's breaches of confidence, Plaintiff
25 and Class Members have been injured and are entitled to damages in an amount to be proven at
26 trial.

27
28 250. Plaintiff seek all monetary and non-monetary relief allowed by law.

COUNT VIII
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT,
CAL. PENAL CODE §§ 631, *et seq.*
(On Behalf of Plaintiff and the California subclass)

251. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

252. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.* declaring that:

advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

The Legislature by this chapter intends to protect the right of privacy of the people of this state.

Cal. Penal Code § 630.

253. To establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant, “by means of any machine, instrument, contrivance, or in any other manner,” does any of the following:

Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,

Or

Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,

Or

Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,

1 Or

2 Aids, agrees with, employs, or conspires with any person or persons to unlawfully
3 do, or permit, or cause to be done any of the acts or things mentioned above in this
4 section.

5 254. Section 631(a) is not limited to phone lines, but also applies to “new technologies”
6 such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21
7 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new technologies” and must be construed broadly to
8 effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134,
9 at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs “electronic communications”); *In re Facebook,*
10 *Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and
11 common law privacy claims based on Facebook’s collection of consumers’ Internet browsing
12 history); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) (“Though
13 written in terms of wiretapping, Section 631(a) applies to Internet communications.”).
14

15 255. Defendant’s website and the tracking technologies Defendant intentionally installed
16 on it are prohibited, as they constitute a “machine, instrument, contrivance, or ... other manner”
17 used to engage in the prohibited conduct at issue here.
18

19 256. All alleged communications between individual Plaintiff or Class Members and
20 Defendant qualify as protected communications under CIPA because each communication is made
21 using personal computing devices (e.g., computers, smartphones, tablets) that send and receive
22 communications in whole or in part through the use of facilities used for the transmission of
23 communications aided by wire, cable, or other like connections.
24

25 257. CCPA and CIPA are complementary statutes. CCPA states that “law relating to
26 consumers’ personal information should be construed to harmonize with the provisions of this
27 title.” Cal. Civ. Code § 1798.175. CCPA further explicitly states that “in the event of a conflict
28

1 between other laws and the provisions of this title, the provisions of the law that afford the greatest
2 protection for the right of privacy for consumers shall control.” *Id.* The ‘opt-out requirements’
3 under the CCPA apply in this online context.
4

5 258. As alleged in the preceding paragraphs, by use of tracking technology, Defendant
6 used a recording device to record the confidential communications in transit including
7 communications or Disclosed Information without the consent of Plaintiff or Class Members and
8 then transmitted such information to Third Parties for Third Party (and fourth party) use.
9

10 259. At all relevant times, Defendant’s aiding of Third Parties to learn the contents of
11 communications and Defendant’s recording of confidential communications was without
12 Plaintiff’s and the Class Members’ authorization and consent.

13 260. Plaintiff and Class Members had a reasonable expectation of privacy regarding the
14 confidentiality of their communications with Defendant. Defendant had duties under statutory and
15 common law to safeguard visitors communications and/or Disclosed Information, and not disclose
16 it without authorization. Defendant never received any authorization and disclosed Plaintiff’s and
17 the Class’s communications or Disclosed Information regardless.
18

19 261. Defendant engaged in and continued to engage in interception by aiding others
20 (including The Trade Desk and Google) to secretly record the contents of Plaintiff’s and Class
21 Members’ wire communications.
22

23 262. The intercepting devices used in this case include, but are not limited to:

- 24 a. Those to which Plaintiff’s and Class Members’ communications were disclosed;
- 25 b. Plaintiff’s and Class Members’ personal computing devices;
- 26 c. Plaintiff’s and Class Members’ web browsers;
- 27 d. Plaintiff’s and Class Members’ browser-managed files;
- 28

- e. Trackers like the Meta Pixel;
- f. Internet cookies;
- g. Other pixels, trackers, and/or tracking technology installed on Defendant's Website and/or server;
- h. Defendant's computer servers;
- i. Third Party source code utilized by Defendant; and
- j. Third Party computer servers (including Facebook).

263. Defendant aided in the interception of contents in that the data from the communications between Plaintiff and/or Class Members and Defendant that were redirected to and recorded by the Third Parties include information which identifies the parties to each communication, their existence, and their contents.

264. Plaintiff and Class Members reasonably expected that their Personal and Financial Information was not being intercepted, recorded, and disclosed to Third Parties or used by Third Parties (and fourth parties) for marketing and profit.

265. No legitimate purpose was served by Defendant's willful and intentional disclosure of Plaintiff's and Class Members' Personal and Financial Information to Third Parties. Neither Plaintiff nor Class Members consented to the disclosure of their Personal and Financial Information by Defendant to Third Parties or the use of the Personal and Financial Information by Third Parties (and fourth parties).

266. The trackers that Defendant utilized are designed such that they transmitted each of a website user's actions to Third Parties alongside and contemporaneously with the user initiating the communication. Thus, Plaintiff's and Class Members' communications were intercepted in transit to the intended recipient (Defendant) before they reached Defendant's servers.

1 267. Defendant willingly facilitated the Third Parties' interception and collection of
2 Plaintiff's and Class Members' Personal and Financial Information, and the Third Parties' (and
3 fourth parties') use of their Personal and Financial Information, by embedding trackers on its
4 Website. Moreover, Defendant had full control over these trackers, including which webpages
5 contained the pixels, what information was tracked and shared, and how events were categorized
6 prior to transmission.
7

8 268. Defendant gave substantial assistance to Third Parties in violating the privacy rights
9 of Mr. Cooper's Customers, even though Defendant's conduct constituted a breach of the
10 confidentiality duties that it owed, including the duty financial institutions owe to their customers
11 and customers' property. Defendant knew that the installation of trackers on its website would
12 result in the unauthorized disclosure of its Customers' communications to Third Parties, and Third
13 Party (and fourth party) use of those communications, yet nevertheless did so anyway.
14

15 269. Plaintiff's and Class Members' electronic communications were intercepted during
16 transmission, without their consent, for the unlawful and/or wrongful purpose of monetizing their
17 Personal and Financial Information, including using their Personal and Financial Information to
18 develop marketing and advertising strategies.
19

20 270. The Personal and Financial Information that Defendant assisted Third Parties with
21 reading, learning, and exploiting, included Plaintiff's and Class Members' Personal and Financial
22 Information customers input into and accessed on Mr. Cooper's Website. Mr. Cooper disclosed
23 details about Customers, like Plaintiff and Class Personal and Financial Information and their
24 interactions with Mr. Cooper's website as users applied for or managed their mortgages, including
25 the fact that a user was on a certain page, that users clicked buttons and what URLs or webpages
26 they led to, the Customer's refinancing options and the user's selections, the state in which the
27
28

property was located, type of property, and the reason the customer was seeking to refinance.

271. Plaintiff and the Class Members seek statutory damages under Cal. Penal Code § 637.2(a), which provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Classes in an amount to be proven at trial, as well as injunctive or other equitable relief.

272. In addition to statutory damages, Defendant's violations caused Plaintiff and Class Members the following damages.

- a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private.
- b. Defendant eroded the essential confidential nature of the mortgagee-mortgagor relationship.
- c. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;
- d. Plaintiff and Class Members did not get the full value of the financial services for which they paid, which included Defendant's duty to maintain confidentiality; and
- e. Defendant's actions diminished the value of Plaintiff's and Class Members' Personal and Financial Information.

273. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT IX
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT,
CAL. PENAL CODE §§ 632, *et seq.*
(On Behalf of Plaintiff and the California subclass)

274. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

1 275. CIPA § 632(a) prohibits an entity from intentionally and without the consent of all
2 parties to a confidential communication, uses an electronic amplifying or recording device to
3 eavesdrop upon or record the confidential communication, whether the communication is carried
4 on among the parties in the presence of one another or by means of a telegraph, telephone, or other
5 device, except a radio.
6

7 276. As alleged in the preceding paragraphs, by use of tracking technology, Defendant
8 used a recording device to record the confidential communications including Disclosed
9 Information without the consent of Plaintiff or Class Members and then transmitted such
10 information to Third Parties for Third Party (and fourth party) use.
11

12 277. At all relevant times, Defendant's aiding of Third Parties to learn the contents of
13 communications and Defendant's recording of confidential communications was without
14 Plaintiff's and the Class Members' authorization and consent.
15

16 278. Plaintiff and Class Members had a reasonable expectation of privacy regarding the
17 confidentiality of their communications with Defendant. Defendant had duties under statutory and
18 common law to safeguard visitors' communications and Disclosed Information, and not disclose
19 it without authorization. Defendant never received any authorization and disclosed Plaintiff's and
20 the Class's communications and Disclosed Information regardless.
21

22 279. Defendant engaged in and continued to engage in interception by aiding others
23 (including The Trade Desk and Google) to secretly record Plaintiff's and Class Members' wire
24 communications.
25

26 280. The intercepting devices used in this case include, but are not limited to:

- 27 k. Those to which Plaintiff's and Class Members' communications were disclosed;
28 l. Plaintiff's and Class Members' personal computing devices;

- m. Plaintiff's and Class Members' web browsers;
- n. Plaintiff's and Class Members' browser-managed files;
- o. Trackers like the Meta Pixel;
- p. Internet cookies;
- q. Other pixels, trackers, and/or tracking technology installed on Defendant's Website and/or server;
- r. Defendant's computer servers;
- s. Third Party source code utilized by Defendant; and
- t. Third Party computer servers (including Facebook).

281. Defendant aided in the interception of contents in that the data from the communications between Plaintiff and/or Class Members and Defendant that were redirected to and recorded by the Third Parties include information which identifies the parties to each communication, their existence, and their contents.

282. Plaintiff and Class Members reasonably expected that their Personal and Financial Information was not being intercepted, recorded, and disclosed to Third Parties or used by Third Parties (and fourth parties) for marketing and profit.

283. No legitimate purpose was served by Defendant's willful and intentional disclosure of Plaintiff's and Class Members' Personal and Financial Information to Third Parties. Neither Plaintiff nor Class Members consented to the disclosure of their Personal and Financial Information by Defendant to Third Parties or the use of the Personal and Financial Information by Third Parties (and fourth parties).

284. The trackers that Defendant utilized are designed such that they transmitted each of a website user's actions to Third Parties alongside and contemporaneously with the user initiating

1 the communication. Thus, Plaintiff's and Class Members' communications were intercepted in
2 transit to the intended recipient (Defendant) before they reached Defendant's servers.

3
4 285. Defendant willingly facilitated the Third Parties' interception and collection of
5 Plaintiff's and Class Members' Personal and Financial Information, and the Third Parties' (and
6 fourth parties') use of their Personal and Financial Information, by embedding trackers on its
7 Website. Moreover, Defendant had full control over these trackers, including which webpages
8 contained the pixels, what information was tracked and shared, and how events were categorized
9 prior to transmission.

10
11 286. Defendant gave substantial assistance to Third Parties in violating the privacy rights
12 of Mr. Cooper's Customers, even though Defendant's conduct constituted a breach of the
13 confidentiality duties that it owed, including the duty financial institutions owe to their customers
14 and customers' property. Defendant knew that the installation of trackers on its website would
15 result in the unauthorized disclosure of its Customers' communications to Third Parties, and Third
16 Party (and fourth party) use of those communications, yet nevertheless did so anyway.

17
18 287. Plaintiff's and Class Members' electronic communications were intercepted during
19 transmission, without their consent, for the unlawful and/or wrongful purpose of monetizing their
20 Personal and Financial Information, including using their Personal and Financial Information to
21 develop marketing and advertising strategies.

22
23 288. The Personal and Financial Information that Defendant assisted Third Parties with
24 reading, learning, and exploiting, included Plaintiff's and Class Members' Personal and Financial
25 Information customers input into and accessed on Mr. Cooper's Website. Mr. Cooper disclosed
26 details about Customers, like Plaintiff and Class Personal and Financial Information and their
27 interactions with Mr. Cooper's website as users applied for or managed their mortgages, including
28

1 the fact that a user was on a certain page, that users clicked buttons and what URLs or webpages
2 they led to, the Customer's refinancing options and the user's selections, the state in which the
3 property was located, type of property, and the reason the customer was seeking to refinance.

4
5 289. Plaintiff and the Class Members seek statutory damages under Cal. Penal Code §
6 637.2(a), which provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount
7 of damages sustained by Plaintiff and the Classes in an amount to be proven at trial, as well as
8 injunctive or other equitable relief.

9
10 290. In addition to statutory damages, Defendant's violations caused Plaintiff and Class
11 Members the following damages.

- 12 a. Sensitive and confidential information that Plaintiff and Class Members intended to remain
13 private is no longer private.
- 14 b. Defendant eroded the essential confidential nature of the mortgagee-mortgagor
15 relationship.
- 16 c. Defendant took something of value from Plaintiff and Class Members and derived benefit
17 therefrom without Plaintiff's and Class Members' knowledge or informed consent and
18 without sharing the benefit of such value;
- 19 d. Plaintiff and Class Members did not get the full value of the financial services for which
20 they paid, which included Defendant's duty to maintain confidentiality; and
- 21 e. Defendant's actions diminished the value of Plaintiff's and Class Members' Personal and
22 Financial Information.
- 23
24

25 291. Plaintiff and Class Members also seek such other relief as the Court may deem
26 equitable, legal, and proper.

27

28 **COUNT X**
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT,

CAL. PENAL CODE §§ 638.51, *et seq.*
(On Behalf of Plaintiff and the California subclass)

292. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

293. CIPA § 638.51 prohibits the installation or use of “a pen register or trap and trace device without first obtaining a court order.” Cal. Penal Code § 638.51(a).

294. Defendant repeatedly violated CIPA § 638.51(a) by installing and using the Trackers without a court order and without any valid consent from users. No valid consent was obtained. Instead, Defendant relied on a knowingly deceptive interface that falsely conveyed user control while continuing to intercept and transmit private communications.

295. An “electronic communication” is defined as “any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system[.]” Cal. Penal Code § 629.51(a)(2).

296. All communications between individual Plaintiff or Class Members and Defendant qualify as protected communications under CIPA because each communication is made using personal computing devices (e.g., computers, smartphones, tablets) that send and receive communications in whole or in part through the use of facilities used for the transmission of communications aided by wire, cable, or other like connections.

297. California Penal Code § 638.50(b) defines a “pen register” as “a device or process that records or decodes dialing, routing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication.”

298. The Trackers are “pen registers” under § 638.50(b) of CIPA because they record “routing, addressing, or signaling information” transmitted by the devices of visitors to Defendant’s website. Cal. Penal Code § 638.50(b).

299. California Penal Code § 638.50(c) defines a “trap and trace device” as “a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication.”

300. The Trackers are also “trap and trace devices” under CIPA § 638.50(c) because they “capture the incoming electronic or other impulses that identify . . . dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication[.]” Cal. Penal Code § 638.50(c).

301. During the Class Period, Defendant installed the Trackers on its website and used them to capture and transmit addressing information, including Plaintiff’s and Class Members’ IP addresses and other unique identifiers to Third Parties.

302. Plaintiff and Class Members did not provide their consent prior to Defendant’s installation and use of the Trackers. On information and belief, Defendant also did not obtain a court order to install or use the Trackers.

303. Under California Penal Code § 637.2, Plaintiff and Class members have been injured by Defendant’s violations of California Penal Code § 638.51(a), and each seek statutory damages of \$5,000 per violation.

304. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT XI
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (“ECPA”)
18 U.S.C. §§ 2511(1), *et seq.*
(On Behalf of Plaintiff, the Nationwide Class, and the California Subclass)

305. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

306. The ECPA protects both sending and receipt of communications. 18 U.S.C. §

1 2520(a) provides a private right of action to any person whose wire or electronic communications
2 are intercepted, disclosed, or intentionally used in violation of Chapter 119.

3
4 307. The transmissions of Plaintiff's and Class Members' Personal and Financial
5 Information to Defendant's Website qualifies as a "communication" under the ECPA's definition
6 of 18 U.S.C. § 2510(12).

7 308. **Electronic Communications.** The transmission of Personal and Financial
8 Information between Plaintiff and Class Members and Defendant's Website with which they chose
9 to exchange communications are "transfer[s] of signs, signals, writing,...data, [and] intelligence
10 of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic,
11 or photo optical system that affects interstate commerce" and are therefore "electronic
12 communications" within the meaning of 18 U.S.C. § 2510(2).
13

14 309. **Content.** The ECPA defines content, when used with respect to electronic
15 communications, to "include [] any information concerning the substance, purport, or meaning of
16 that communication." *See* 18 U.S.C. § 2510(8).
17

18 310. **Interception.** The ECPA defines the interception as the "acquisition of the contents
19 of any wire, electronic, or oral communication through the use of any electronic, mechanical, or
20 other device" and "contents...include any information concerning the substance, purport, or
21 meaning of that communication." *See* 18 U.S.C. § 2510(4), (8).
22

23 311. **Electronic, Mechanical or Other Device.** The ECPA defines "electronic,
24 mechanical, or other device" as "any device...which can be used to intercept a[n]...electronic
25 communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning
26 of 18 U.S.C. § 2510(5):
27

- 28 a. Plaintiff's and Class Members' browsers;

- b. Plaintiff's and Class Members' computing devices;
- c. Defendant's web-servers;
- d. Defendant's Website; and
- e. The tracking technology deployed by Defendant effectuated the sending and acquisition of customer communications.

312. By utilizing and embedding the tracking technology on its Website, Defendant intentionally intercepted, endeavored to intercept and procured another person to intercept the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

313. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the tracking technology which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' Personal and Financial Information to Third Parties.

314. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiff and Class Members regarding Personal and Financial Information.

315. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to Third Parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

316. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

317. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of

1 Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious
 2 act in violation of the Constitution or laws of the United States or of any State – namely, invasion
 3 of privacy, among others.
 4

5 318. Defendant intentionally used the wire or electronic communications to increase its
 6 profit margins and save on marketing costs.

7 319. Defendant specifically used tracking technology to track and to utilize Plaintiff's
 8 and Class Members' Personal and Financial Information for financial gain.

9 320. Defendant was not acting under color of law to intercept Plaintiff's and Class
 10 Members' wire or electronic communication.
 11

12 321. Plaintiff and Class Members did not authorize Defendant to acquire the content of
 13 their communications for purposes of invading Plaintiff's and Class Members' privacy via the
 14 tracking technology.
 15

16 322. In sending and in acquiring the content of Plaintiff's and Class Members'
 17 communications relating to the browsing of its Website, Defendant's purpose was tortious,
 18 criminal and designed to violate federal and state legal provisions, including as described above
 19 the following: (i) a knowing intrusion into a private, place, conversation or matter that would be
 20 highly offensive to a reasonable person; and (ii) violation of GLBA, the FTC Act, invading
 21 Plaintiff's and Class Members' privacy, and in breach of its fiduciary duty of confidentiality.
 22

23 **COUNT XII**
 24 **VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT**
 25 **18 U.S.C. § 2511(3)(a)**
 26 **UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE**
 27 **(On Behalf of Plaintiff, the Nationwide Class, and the California Subclass)**

28 323. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

324. The ECPA statute provides that “a person or entity providing an electronic

1 communication service to the public shall not intentionally divulge the contents of any
2 communication (other than one to such person or entity, or an agent thereof) while in transmission
3 on that service to any person or entity other than an addressee or intended recipient of such
4 communication or an agent of such addressee or intended recipient.” 18 U.S.C. § 2511(3)(a).

6 **325. Electronic Communication Service.** An “electronic communication service” is
7 defined as “any service which provides to users thereof the ability to send or receive wire or
8 electronic communications.” 18 U.S.C. § 2510(15). Defendant’s Website is an electronic
9 communication service which provides to users thereof, customers of Defendant, the ability to
10 send or receive electronic communications; in the absence of Defendant’s Website, internet users
11 could not send or receive communications regarding Plaintiff’s and Class Members’ Personal and
12 Financial Information.

14 **326. Intentional Divulgence.** Defendant intentionally designed the tracking technology
15 and was or should have been aware that, if so configured, it could divulge Plaintiff’s and Class
16 Members’ Personal and Financial Information. Upon information and belief, Defendant’s
17 divulgence of the contents of Plaintiff’s and Class Members’ communications was
18 contemporaneous with their exchange with Defendant’s Website, to which they directed their
19 communications.

21 **327.** Defendant divulged the contents of Plaintiff’s and Class Members’ electronic
22 communications without authorization and/or consent.

24 **328. Exceptions do not apply.** In addition to the exception for communications directly
25 to an electronic communications service (“ECS”)⁶⁷ or an agent of an ECS, the ECPA states that
26

27
28 ⁶⁷ An ECS is “any service which provides to users thereof the ability to send or receive
wire or electronic communications.” 18 U.S.C. § 2510(15).

[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication”...“as otherwise authorized in section 2511(2)(a) or 2517 of this title; “with the lawful consent of the originator or any addressee or intended recipient of such communication;” c. “to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;” or d. “which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

U.S.C. § 2511(3)(b).

329. Section 2511(2)(a)(i) provides:

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

330. Defendant’s divulgence of the contents of Plaintiff’s and Class Members’ communications to Facebook, Google, and Microsoft was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (i) a necessary incident to the rendition of Defendant’s service nor (ii) necessary to the protection of the rights or property of Defendant.

331. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

332. Defendant’s divulgence of the contents of Plaintiff’s and the Class Members’ communications on its Website through the tracking technology was not done “with the lawful consent of the originator or any addresses or intended recipient of such communication[s].” As alleged above: (i) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications and (ii) Defendant did not procure the “lawful consent” from the websites or apps with which Plaintiff and Class Members were exchanging information.

1 333. Moreover, Defendant divulged the contents of Plaintiff's and Class Members'
2 communications through tracking technology to individuals who are not "person[s] employed or
3 whose facilities are used to forward such communication to its destination."
4

5 334. The contents of Plaintiff's and Class Members' communications did not appear to
6 pertain to the commission of a crime and Defendant did not divulge the contents of their
7 communications to a law enforcement agency.
8

9 335. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may
10 assess statutory damages, preliminary and other equitable or declaratory relief as may be
11 appropriate, punitive damages in an amount to be determined by a jury and a reasonable attorney's
12 fee and other litigation costs reasonably incurred.

13 **PRAYER FOR RELIEF**

14 **WHEREFORE**, Plaintiff, individually and on behalf of all others similarly situated, pray
15 for judgment as follows:
16

- 17 A. For an Order certifying this action as a Class action and appointing Plaintiff as Class
18 Representatives and Plaintiff's counsel as Class Counsel;
- 19 B. For an award of actual damages, compensatory damages, statutory damages, and
20 statutory penalties, in an amount to be determined, as allowable by law;
- 21 C. For an award of punitive damages, as allowable by law;
- 22 D. For equitable relief enjoining Defendant from engaging in the wrongful conduct
23 complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and
24 Class Members' Personal and Financial Information and from refusing to issue
25 prompt, complete and accurate disclosures to Plaintiff and Class Members;
26
27
28

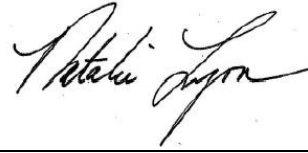
- 1 E. For an Order declaring the rights and obligations of the parties, including, without
2 limitation, that Defendant owes a legal duty to its Customers to secure their
3 Personal and Financial Information and that Defendant violates this legal duty by
4 disclosing its Customers' Personal and Financial Information to unaffiliated Third
5 Parties;
6
- 7 F. For equitable relief compelling Defendant to utilize appropriate methods and
8 policies with respect to consumer data collection, storage, and safety and to disclose
9 with specificity the type of Personal and Financial Information compromised and
10 unlawfully disclosed to Third Parties;
11
- 12 G. For equitable relief requiring restitution and disgorgement of the revenues
13 wrongfully retained as a result of Defendant's wrongful conduct;
14
- 15 H. For an Order compelling Defendant to pay for not less than three years of credit
16 monitoring services for Plaintiff and the Classes;
17
- 18 I. For an award of reasonable attorneys' fees and costs under the laws outlined above,
19 the common fund doctrine, and any other applicable law;
20
- 21 J. Costs and any other expenses, including expert witness fees incurred by Plaintiff in
22 connection with this action;
23
- 24 K. Pre- and post-judgment interest on any amounts awarded; and
25
- 26 L. Such other and further relief as this court may deem just and proper.
27

JURY DEMAND

25 Plaintiff, individually and on behalf of all others similarly situated, hereby demand a trial
26 by jury on all issues so triable.
27

28 Dated: September 8, 2025

Respectfully submitted,



Natalie Lyons, No. 293026
Vess A. Miller, No. 278020
Lynn A. Toops*
Lisa M. La Fornara*
COHENMALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
nlyons@cohenmalad.com
vmiller@cohenmalad.com
ltoops@cohenmalad.com
llaforara@cohenmalad.com

J. Gerard Stranch, IV*
Emily E. Schiller*
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
eschiller@stranchlaw.com

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI, PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
(872) 263-1109 (facsimile)
sam@straussborrelli.com
raina@straussborrelli.com

*To seek admission *pro hac vice*

***Counsel for Plaintiff and the Proposed
Classes***